ALLE DAGEN INTERNET - BEHEERSEN DOOR BEHEREN

REDE UITGESPROKEN BIJ DE AANVAARDING
VAN HET AMBT VAN HOOGLERAAR

NETWORK OPERATIONS AND MANAGEMENT

AAN DE FACULTEIT ELEKTROTECHNIEK, WISKUNDE
EN INFORMATICA VAN DE UNIVERSITEIT TWENTE
OP DONDERDAG 13 NOVEMBER 2014 DOOR

PROF. DR. IR. AIKO PRAS

1. Introductie

MIJNHEER DE RECTOR, BESTE FAMILIE, VRIENDEN EN COLLEGAE

Het is exact 35 jaar geleden dat ik aan de THT begon bij de vakgroep Digital Techniek aan een bacheloropdracht met als onderwerp 'dynamische routering in computernetwerken' [1]. In die tijd was ik nog van plan om af te studeren op het gebied van analoge electronica, zodat ik later een mooie baan bij Philips kon krijgen op de afdeling waar HIFI-versterkers werden gemaakt. Gezien de opkomst van computers leek het me echter verstandig eerst ook iets van 'digitale technieken' te leren, waarschijnlijk was dergelijke kennis toch wel handig voor mijn latere carrière. Toen ik met mijn bacheloropdracht begon was een van de eerste dingen die mijn toenmalige begeleider Ben van den Dolder tegen mij zei, dat dit vakgebied zo leuk was, dat ik nooit meer wat anders zou doen. Hij heeft gelijk gekregen.

Mijn fascinatie voor computers en vooral computernetwerken is dus 35 jaar oud. Initieel was ik primair geïnteresseerd in het ontwerpen van computernetwerken. Het Internet en het World Wide Web bestonden nog niet, maar ik probeerde mij al voor te stellen hoe de wereld er uit zou zien als we video telefonie en email zouden hebben. In mijn eerste universitaire jaren werkte ik dan ook aan het ontwerp van een lokaal netwerk dat 'TwenteNet' was genoemd. Dit netwerk was in staat maar liefst 16 Megabit per seconde (Mbps) te transporteren; een snelheid die door sommige hoogleraren als onzinnig werd afgedaan, omdat normale mensen toch niet meer dan een paar karakters per seconde konden lezen en schrijven.

Vanaf de tweede helft van de jaren tachtig verschoof mijn interesse geleidelijk van het ontwerp van netwerken naar het gebruik van netwerken en wat er moet gebeuren om netwerken operationeel te houden en te beheren. Ik ben op dit gebied later gepromoveerd en nu als hoogleraar benoemd.

Ook op het gebied van netwerkbeheer zijn er veel nieuwe ontwikkeling geweest. Initieel is er veel onderzoek uitgevoerd op het gebied van managementarchitecturen en -protocollen, zoals het Simple Network Management Protocol (SNMP); ook ik heb aan dergelijke ontwikkelingen meegewerkt.

De laatste jaren ben ik echter vooral gefascineerd door het 'creatieve gebruik' van het Internet, dus gebruik op een manier zoals de ontwerpers nooit voor ogen hebben gehad. Meestal hebben we het dan over misbruik van het Internet, zoals het genereren van zoveel verkeer dat normaal gebruik onmogelijk wordt. Over dit soort 'incidenten' lezen we bijna dagelijks in de krant; ik zal in mijn verhaal daarom met name hierop ingaan.

Ik wil echter eerst iets vertellen over de mindset die nodig is om, in plaats van iets te ontwerpen, een complex systeem zoals het Internet te beheren. Ik zal mij echter beperken tot het geven van een overzicht en niet ingaan op de statistische methoden, Markov modellen, clustering technieken etc. die nodig zijn om op dit interessante onderzoeksgebied resultaten te bereiken. Voor de geïnteresseerden verwijs ik graag naar de diverse artikelen die we op dit vakgebied hebben gepubliceerd.

2. Ontwerp versus Beheer

Een groot deel van mijn collegae binnen de afdelingen informatica en elektrotechniek richten zich in hun onderzoek op het ontwerpen van nieuwe systemen. In de beginjaren werkte men vooral aan het ontwerpen van computersystemen, besturingssystemen, databases, netwerken enz. Tegenwoordig heeft men zich vaak verder gespecialiseerd en werkt men ook aan het ontwerp van embedded systems, distributed systems, pervasive systems, car-to-car systems, information systems, secure systems, robotic systems etc. Onderzoek op deze gebieden heeft vaak een vergelijkbare systematiek en kan in drie fases worden opgedeeld:

1. formulering van de ontwerpeisen
2. ontwerp van het systeem, of de systeemarchitectuur
3. validatie of het systeem aan de ontwerpeisen voldoet. De validatie kan kwalitatief of kwantitatief van aard zijn en gebaseerd zijn op wiskundige modellen, simulaties alsmede metingen aan een prototype.

In veel publicaties van mijn collegae kan men, impliciet of expliciet, deze drie fases terugvinden. Ook zullen zij in het algemeen alle facetten doorzien van het systeem dat ze ontwerpen. Zoals een van mijn leermeesters, Prof. Gerrit Blaauw, aan het eind van de jaren zeventig van de vorige eeuw zo mooi formuleerde: “We believe the notion of a single designer controlling an entire computer architecture is not only practical but in fact essential for good design” [1].

We zijn nu echter 35 jaar verder en veel systemen waar we vroeger alleen van konden dromen zijn nu op grote schaal geïntroduceerd. ICT-systemen bepalen ons dagelijks leven en een maatschappij zonder Internet is niet meer voorstelbaar. Als het Internet op grote schaal zou uitvallen, gaan bedrijven zoals Google, Facebook en Amazon onmiddellijk failliet. Maar ook allerlei andere bedrijven komen in grote problemen. Het betalingssysteem valt stil, omdat electronisch bankieren niet meer meer mogelijk is en alternatieve systemen inmiddels ontmanteld zijn. Aandelen kunnen niet meer verhandeld worden en beurskoersen storten in. Winkels worden niet meer

bevoorraad en eten wordt schaars. Om een analogie met de spoorwegstaking van 1903 te gebruiken: “Gansch het raderwerk staat stil, als het Internet niet meer wil”.

Het probleem bij complexe systemen zoals het Internet is echter dat er niemand meer is die alle facetten van het systeem doorziet. Het systeem is zo complex geworden, dat een kleine verandering grote en onvoorziene gevolgen kan hebben. Omdat het voor de samenleving van groot belang is dat het Internet goed blijft functioneren, is onderzoek op het gebied van operationele aspecten en Internetbeheer cruciaal. Dit is dan ook het gebied waar ik mij op richt.

Onderzoek op het gebied van operationele aspecten kent een wat andere systematiek dan het meer op ontwerp gerichte onderzoek van veel van mijn collegae. Mijn eigen onderzoek begint vaak met een hypothese, die aanleiding geeft tot een aantal onderzoeksvragen. Om deze vragen te beantwoorden moeten vaak metingen worden verricht, waarna de hypothese kan worden aangenomen, verworpen of verfijnd.

Een aardig voorbeeld is het onderzoek van één van mijn voormalige promovendi, Giovane Moura, naar zogeheten Internet ‘Bad Neighborhoods’. De hypothese was dat op het Internet, net zoals in de fysieke wereld, bepaalde gebieden bestaan waar relatief vaak ‘slecht gedrag’ wordt vertoond en waartoe je dus beter afstand kan bewaren. Deze hypothese heeft geleid tot een aantal onderzoeksvragen, zoals: waar komt de meeste SPAM vandaan en waar staan de meeste phishing servers. Omdat het begrip ‘gebied’ op het Internet verschillende geïnterpreteerd kan worden, zijn de onderzoeksvragen verfijnd en is gekeken naar gedrag binnen geografische gebieden, dus landen en steden, gedrag binnen subnetwerken met dezelfde IP adres prefix en naar gedrag binnen dezelfde Internet Service Providers (ISPs) en Autonomous Systems (ASs).

Figuur 2.1 laat zien dat SPAM vooral verstuurd wordt vanuit de zogeheten ‘BRIC’ landen (Brazilië, Rusland, India en China). Een mogelijke verklaring hiervoor is dat in die landen

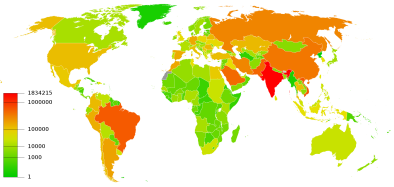

Fig. 2.1: Top Spam countries

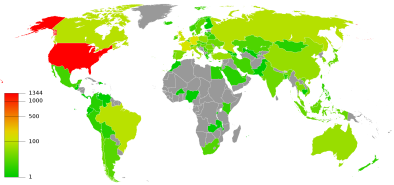

Fig. 2.2: Top Phishing countries

relatief veel computers zijn gehacked en opgenomen in een botnet. In die landen zijn computers pas later op grote schaal ingevoerd en hebben inwoners dus gemiddeld wat minder ervaring met de beveiliging van computers dan in West Europa en de VS. Tevens wordt er waarschijnlijk vaak gewerkt met wat oudere software, die minder goed of zelfs helemaal niet ondersteund wordt, en misschien worden ook wel vaker bestanden uit dubieuze bron gedownload.

Figuur 2.2 laat zien dat phishing servers, dus namaak websites die bijvoorbeeld proberen je bank- en creditcardgegevens te bemachtigen, vooral vanuit de VS opereren. Een mogelijke verklaring hiervoor is dat phishing sites 24 uur per dag bereikbaar moeten zijn, omdat anders personen die op een phishing link klikken onmiddellijk argwaan krijgen als de website van hun bank of creditcardmaatschappij niet bereikbaar is. Phishing sites zijn dus vooral te vinden bij grote bedrijven die veel websites beheren, en die dus vaak in de VS staan.

Uit beide figuren blijkt dat er dus een groot verschil is tussen SPAM en phishing 'Bad Neighborhoods'.

Als het begrip 'gebied' geïnterpreteerd wordt als ISP, dan komen heel andere 'Bad Neighborhoods' naar voren. Tabel 2.1 laat zien bij welke ISPs relatief veel spammers gevonden worden. De eerste positie wordt ingenomen door SpectraNet Limited, een ISP uit Nigeria (NG) die op het moment dat onze metingen werden verricht in totaal slechts 5632 IP-adressen in bezit had. Vanaf bijna 63% van deze adressen (3523 adressen) werd SPAM verstuurd, dus de kans dat een email bericht van deze provider SPAM bevat is relatief hoog.

In ons onderzoek zijn ruim 42 duizend ISPs beschouwd en onze conclusie was dat bijna de helft van alle SPAM afkomstig

#	Ratio (%)	AS Name	Bad IPs	Total IPs	Country
1	62.55	SpectraNet Limited	3,523	5,632	NG
2	55.56	SC Media SUD SRL	1,138	2,048	RO
3	43.77	OJSC MegaFon Network	1,793	4,096	RU
4	40.81	Udyog Vihar	78,992	193,536	IN
5	39.2	SpeedClick for ITC	803	2,048	PS
6	37.03	NetStream Technology	1,517	4,096	PS
7	35.97	Orange Cameroun SA	2,947	8,192	CM
8	35.93	MTC KSA Mobile	552	1,536	SA
9	35.35	Dade Pardazi Novin Yaran Tosei	181	512	IR
10	34.17	Behkoush Rayaneh Afzar Co.	700	2,048	IR

Tabel 2.1: Top Spam ISPs

is vanuit slechts 20 ISPs. Het is dus duidelijk dat deze ISPs als 'Bad Neighborhoods' beschouwd kunnen worden, een gegeven waar tijdens de bouw van SPAM-filters rekening mee gehouden kan worden.

2.1. Meten

Een belangrijke activiteit bij ons onderzoek is het verrichten van metingen aan operationele, dus bestaande systemen. Op een bepaalde manier is ons onderzoek daarom vergelijkbaar met onderzoek op het gebied van de geologie of astronomie; ook daar ligt de nadruk op het observeren van en het meten aan 'bestaande systemen'. Dergelijke metingen kunnen actief of passief van aard zijn. Bij actieve metingen wordt een meetsignaal naar het te onderzoeken systeem gestuurd en vervolgens weer gemeten. Zo kan een geoloog of seismoloog een trilling genereren en uit de tijd die ligt tussen het zenden en ontvangen van het meetsignaal de aard en dikte van een bepaalde aardlaag berekenen. Bij passieve metingen worden

geen speciale meetsignalen verstuurd, maar reeds aanwezige signalen gemeten. Zo kan een astronoom de aanwezigheid van zwarte gaten bepalen door de afbuiging van lichtstralen die worden verstuurd door sterren in de buurt van het zwarte gat te meten.

Net als geologen en astronomen moeten wij bij de analyse van onze metingen grote hoeveelheden data verwerken. De term 'big data' is dus ook op ons onderzoek van toepassing. Voor ons onderzoek analyseren wij data over miljarden 'gebeurtenissen'. De opslagcapaciteit die wij als onderzoeksgroep gebruiken is ruwweg 500 TB, een getal dat vergelijkbaar is met de opslagcapaciteit van de centrale UT-voorzieningen.

Op het Internet zijn er heel veel zaken waaraan gemeten kan worden. Zo kan bijvoorbeeld het gedrag en de belasting van Internetsystemen, zoals servers, routers en switches, gemeten worden; voor het verrichten van dergelijke metingen wordt vaak gebruik gemaakt van het Simple Network Management Protocol (SNMP). In het verleden heeft onze onderzoeksgroep door het bouwen van prototypes aan de ontwikkeling van dit protocol bijgedragen.

Naast het gedrag en de belasting van systemen kan natuurlijk ook gemeten worden aan het verkeer dat over het Internet wordt verstuurd. Initieel was bij dergelijke metingen vooral het doel de kwaliteit van Internetdiensten te monitoren en te verbeteren. Eén aspect hierbij is het bepalen of de capaciteit van bepaalde Internetverbindingen wel voldoende is; als onderzoeksgroep zijn wij reeds geruime tijd vooral op dit gebied actief. Tegenwoordig ligt de nadruk steeds meer op netwerkbeveiliging en wordt het Internetverkeer gemeten om aanvallen te detecteren en te bestrijden.

Er zijn meerdere methoden om het Internetverkeer te meten. Een voor de hand liggende methode is het aansluiten van een meetapparaat, vaak een linux-PC, op een monitorpoort van een router of op een optische tab. Het meetapparaat ontvangt een kopie van ieder verstuurd pakket en slaat dit pakket gedeeltelijk of in zijn geheel op voor latere analyse. Tools die hiervoor vaak gebruikt worden zijn tcpdump en wireshark. Een probleem bij deze methode is dat het meetapparaat vaak

de hoeveelheid pakketten die over een Internetverbinding worden verstuurd niet meer kan bijhouden. Pakket-gebaseerde metingen zijn daarom minder geschikt voor het verrichten van metingen dichter op de kern van het Internet, waar grote hoeveelheden data worden verstuurd. In dergelijke omgevingen is het beter gebruik te maken van flow-based metingen; als onderzoeksgroep zijn we ons rond 2007 in dergelijke metingen gaan specialiseren en zijn ondertussen hierop één van de leidende groepen wereldwijd geworden.

2.2. Flow-based meten

Bij flow-based metingen worden niet de pakketten zelf, maar informatie over pakketstromen bijgehouden. Vergeleken met pakketgebaseerde metingen wordt er bij flow-based metingen slechts een fractie van de data opgeslagen en geanalyseerd; hierdoor is een reductie mogelijk met een factor 2000 [2].

Figuur 2.3 laat zien welke informatie wordt bijgehouden als er bijvoorbeeld data wordt verstuurd van systeem A naar B:
- Het aantal pakketten dat is verstuurd (100 pakketten).
- Het totaal aantal bytes dat is verstuurd (95310 bytes).
- Hoe laat het eerste pakket is verstuurd (13:56).

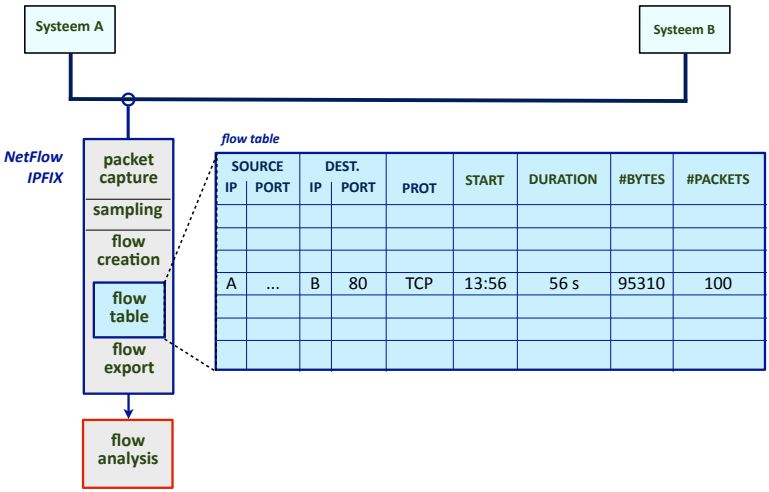

Fig. 2.3: Voorbeeld van Flow-based metingen

- Hoe lang de communicatie heeft geduurd (56 seconde).
- De IP-adressen waartussen informatie is uitgewisseld (van A naar B).
- Tussen welke poorten communicatie heeft plaatsgevonden (er is gecommuniceerd naar poort 80; deze poort wordt gebruikt voor webverkeer).
- Welk protocol is gebruikt (TCP).

Bovenstaande informatie wordt bijgehouden in het geval van NetFlow versie 5, een veel gebruikte technologie die in alle professionele routers van Cisco is ingebouwd. Moderne Cisco-routers implementeren NetFlow versie 9, waarmee het mogelijk is nog veel meer meta-informatie te verzamelen. De Internet Engineering Task Force (IETF) heeft NetFlow V9 als basis genomen voor IPFIX, een norm voor flow-based meten die door veel fabrikanten wordt ondersteund.

Flow-based meten heeft dus vele voordelen. Ten opzichte van het traditionele pakketgebaseerd meten is de hoeveelheid te analyseren data gereduceerd met een factor 2000; door gebruik te maken van sampling-technieken kan een nog verdere reductie bereikt worden. De verzamelde meta-data is identiek aan de data die moet worden opgeslagen om aan de Europese 'data retention laws' te voldoen. Flow-based technologie wordt door veel fabrikanten ondersteund en is beschikbaar bij 70% van alle netwerkoperators [3]. Omdat er alleen meta-data, maar geen gebruikersdata, zoals bijvoorbeeld creditcard-gegevens, wordt opgeslagen, zijn er minder problemen voor wat betreft privacy. Tevens worden metingen niet verstoord indien de gebruikersdata wordt versleuteld.

3. Network security

Er gaat bijna geen dag voorbij of er wordt in de media wel melding gemaakt van een Internetaanval. Alhoewel de schade van dergelijke aanvallen moeilijk is te becijferen, worden voor Nederland getallen genoemd van meerdere miljarden euros per jaar [4]. Onderzoek op het gebied van Internet-security en de schade die door cyberaanvallen wordt veroorzaakt is dan ook van groot economisch en maatschappelijk belang. Ik ben dan ook blij dat de UT op dit gebied voorop loopt; niet alleen op mijn eigen terrein, dus de detectie en preventie van Internetaanvallen, maar ook op andere terreinen, zoals beveiliging van SCADA-systemen, socio-technical risk management, intelligent surveillance, alsmede ethische aspecten. Samenwerking op dit gebied is cruciaal: op CTIT-niveau binnen één van de Research Centres; en op UT niveau tussen het CTIT, IGS en de Twente Safety & Security Region.

Aanvallen op het Internet kunnen ruwweg door drie partijen worden uitgevoerd: 1) script-kiddies, 2) de georganiseerde misdaad en 3) veiligheidsdiensten. Hoewel onze onderzoeksgroep zich vooral richt op de eerste groep, wil ik de rol van veiligheidsdiensten eerst bespreken.

3.1. Veiligheidsdiensten

Het feit dat Veiligheidsdiensten een bedreiging voor de veiligheid op het Internet vormen klinkt en is paradoxaal. Het probleem is echter dat veiligheidsdiensten de neiging hebben alles te willen weten ('big-brother is watching you') en dat acties die voor de ene partij voor veiligheid moeten zorgen bij de andere partij juist tot onveiligheid leiden. Als het ene land alles weet over het andere land, is dat prettig voor dat ene land, maar bedreigend voor het andere land. Dat veiligheidsdiensten er niet voor terugdeinzen regeringsleiders van bevriende landen af te luisteren is bij het grote publiek ten minste bekend sinds de afluisteraffaire rond Bondskanselier Merkel. Minder bekend zijn activiteiten zoals HACIENDA, een programma van de Angelsaksische veiligheidsdiensten die alle systemen op het Internet systematisch afzoekt met als doel

zoveel mogelijk gegevens te verzamelen. Deze gegevens worden later gebruikt om gericht in te breken. In principe moet op iedere computer ingebroken kunnen worden; iedere Internetgebruiker is in principe verdacht en moet dus bespioneerd kunnen worden. Om dergelijke activiteiten te versluieren wordt door sommige veiligheidsdiensten eerst ingebroken op een groot aantal gewone computers, zogeheten Operational Relay Boxes (ORBs), die vervolgens weer gebruikt worden voor het verder afzoeken van het Internet [5]. Een dergelijk netwerk van gehackte systemen staat bekend als botnet; ook criminelen maken gebruik van botnets en dergelijk gebruik is strafbaar.

Nadat het hele Internet in kaart is gebracht, kan gericht worden ingebroken op systemen door gebruik te maken van bekende zwakheden, of nog onbekende zwakheden, zogeheten zero-day exploits. Zo werd eerder dit jaar een fout bekend in de implementatie van het OpenSSL/TLS protocol, waardoor het mogelijk werd om tussen een kwart en de helft van alle webservers wereldwijd in te breken en passwords van gebruikers te onderscheppen [6]. De fout die bekend staat onder de naam Heartbleed werd in April 2014 bekend, maar volgens persbureau Bloomberg al sinds twee jaar gebruikt door de Amerikaanse veiligheidsdienst NSA, die dit overigens ontkent [7]. Over de hele wereld werden gebruikers van online diensten gevraagd hun passwords aan te passen; de kosten voor het herstellen van deze fout wordt door sommigen geraamd op een half miljard dollar [8].
Het gebruik van zero-day exploits is overigens niets nieuws; het bekende Stuxnet virus uit 2010 om het Iraanse uraniumverrijkingsprogramma te saboteren bevatte zelfs 4 zero-day exploits.

Gevaarlijker voor de veiligheid van burgers, bedrijven en instellingen is echter het bewust toevoegen van software of het inbouwen van fouten, met het doel later makkelijker via zogeheten backdoors te kunnen inbreken. Dergelijke backdoors kunnen namelijk niet alleen door de eigen veiligheidsdienst, maar ook door andere diensten en criminelen worden gebruikt. Het inbouwen van backdoors door veiligheidsdiensten wordt meestal ontkend, maar in 2011 moest de Beierse

regering toegeven dat ze zelf actief computers infecteerde [9]. De spionage-software, die al snel de bijnaam 'Staatstrojaner' kreeg, was dusdanig slecht gebouwd dat het door iedere student met enige kennis van ICT kon worden misbruikt. 'Bewijs' dat de veiligheidsdienst door deze backdoor hoopte te vergaren kon dus makkelijk door derden worden gemanipuleerd.
Het is, zeker na de Snowdon-publicaties, aannemelijk dat ook de Amerikaanse veiligheidsdienst op grote schaal bewust backdoors inbouwt en beveiligingssoftware zoals SSL verzwakt [10][11]. In het kader van het PRISM-programma wordt door de NSA de communicatie bij bedrijven zoals Microsoft, Google, Facebook, Skype, AOL en Apple afgetapt [12]. Ook zijn er aanwijzingen dat de Amerikaanse veiligheidsdienst, als onderdeel van het zogeheten TURBINE programma, zelf een aantal fake Facebook-servers gebruikt om computers, men praat over een miljoen, van malafide software te voorzien [13].

Niet alleen westerse, maar ook Chinese, Russische, Iraanse en andere veiligheidsdiensten zijn op grote schaal actief met het hacken en infiltreren van computersystemen. Om Carl von Clausewitz te parafraseren: "Der Cyberkrieg ist eine bloße Fortsetzung der Politik mit anderen Mitteln" [14]. Toch is het, in een maatschappij waarin politici en beleidsmakers geconfronteerd worden met nieuwe technologieën waarvan ze weinig kaas hebben gegeten, niet vreemd dat er uitwassen ontstaan waarin de zogenaamde 'veiligheid van de staat' een boven proportionele rol gaat spelen. Reeds in 1847, toen de Hollandsche IJzeren Spoorweg-Maatschappij (HIJSM) toestemming vroeg haar telegraaflijn ook voor het publiek open te stellen, werden "om uit te sluiten dat de telegraaf voor snelle en criminele acties zou worden gebruikt", telegraafkantoren verplicht registers bij te houden "waarin de tekst van ieder telegram wordt opgeschreven". De burgermeester dient "het register regelmatig te controleren en van zijn paraaf te voorzien". In het 'Reglement voor de dienst van den Rijks-telegraaf' uit 1854 werd "voor particulieren het gebruik van geheimschrift verboden" [15]. Een paar jaar later werden deze onzinnige regels afgeschaft, nadat politici en beleidsmakers iets meer gingen begrijpen van het medium telegraaf. De hoop is dat ook nu, nadat politici en beleidsmakers iets meer gaan begrijpen van

het medium Internet, betere wetten opgesteld worden om de activiteiten van veiligheidsdiensten te reguleren.

Concreet stel ik voor dat het per wet verboden moet worden dat veiligheidsdiensten *onbeperkt* gegevens verzamelen over *alle* op het Internet aangesloten systemen en dat ze zonder *rechterlijke goedkeuring* niet op willekeurige Internetsystemen mogen inbreken. Ook moeten veiligheidsdiensten verplicht worden eventueel door hen gevonden veiligheidsproblemen, waaronder zero-day exploits, te melden, zodat zoveel mogelijk beveiligingsgaten gedicht worden [16]. Veiligheidsdiensten moeten primair als taak hebben de veiligheid van burgers en bedrijven te vergroten, en niet hun eigen kennis en macht.

Ik wil er ook voor pleiten dat overheden structureel gaan meebetalen aan de ontwikkeling en onderhoud van cruciale Internetsoftware. Zo wordt het eerder genoemde OpenSSL/TLS protocol onderhouden door slechts een paar vrijwilligers op basis van giften met een totale waarde van enige duizenden dollars; onvoldoende om hun elektriciteitsrekening te betalen [17]. Tegelijkertijd hebben veiligheidsdiensten grote aantallen onderzoekers in dienst en hebben ze budgetten van miljarden dollars die ze kunnen besteden om veiligheidslekken in Internetsoftware op te sporen [18].

3.2. Privacy

Niet alleen overheden moeten de nieuwe regels van het Internet beter leren begrijpen, maar zeker ook de gewone burgers, bedrijven en instellingen. Om een parallel te trekken, we denken nog net zoals de dorpsbewoners van ruim een eeuw geleden die vanuit de armste plattelandsgebieden in Europa vertrokken naar een nieuwe toekomst in de grote stad New York. We dachten dat ook in de grote stad New York dezelfde regels golden als op het platteland. We deden de huisdeur niet op slot, want niemand zou wat stelen en we hadden toch niets te verbergen.

Vandaag, ruim een eeuw later, is er weinig veranderd. Bij veel burgers ontbreekt nog steeds het besef dat buitenstaanders via de Internetaansluiting thuis waardevolle informatie kunnen ontvreemden. De Internetaansluiting is echter niet

vergelijkbaar met de gas-, water- en elektriciteitaansluitingen, die nauwelijks door derden te misbruiken zijn. Als ik jongeren vraag waarom ze zoveel privé-gegevens op Facebook zetten, dan krijg ik als antwoord dat ze toch niets van waarde te verbergen hebben. Ze vergeten echter dat ogenschijnlijk onschuldige informatie, zoals het lijstje met vrienden of het adresboek, nu al door bedrijven gebruikt wordt om de kredietwaardigheid van individuen te bepalen. Een aantal banken maakt al gebruik van dergelijke informatie: als je vrienden hebt die schulden hebben krijg je mogelijk zelf geen hypotheek. Als er veel ziektes in je familie voorkomen krijg je mogelijk geen levensverzekering.

Niet alleen burgers, maar ook bedrijven en instellingen moeten nog aan de nieuwe regels van cyberspace wennen. Als TNT post al onze brieven zou openmaken om nuttige informatie aan derden te verkopen, dan zou dat een schandaal zijn. Als een universiteit email van studenten en medewerkers aan Google uitbesteedt, die vervolgens alle emails gaat scannen op nuttige informatie, dan zijn we blij, omdat we geld voor eigen mailservers hebben bespaard. Dat bedrijven zoals Google miljarden verdienen aan de verkoop van onze informatie kunnen we ons echter maar moeilijk voorstellen. Dergelijke bedrijven kunnen echter profielen opstellen welke studenten goed zijn, wie vaak ziek is, van welke verenigingen een student lid is en door het koppelen van surfgedrag kan bepaald worden welke politieke of andere interesses die student heeft. Potentiële werkgevers willen voor dergelijke informatie graag betalen. Naast email geven universiteiten ook het surfgedrag op hun websites door aan commerciële bedrijven, die hieruit bijvoorbeeld kunnen bepalen wie ontevreden is met zijn huidige werkgever en op zoek is naar een nieuwe baan.

Surfgedrag is dus privacygevoelige informatie. Bij veel mensen leeft echter nog de misvatting dat het in kaart brengen van surfgedrag kan worden tegengegaan door het weigeren van browser cookies. De industrie is echter al mijlen verder en kan door technieken zoals browser fingerprinting en clock skew met grote zekerheid computersystemen en dus gebruikers uniek identificeren, ook als het gaat om laptops die op wisselende plaatsen worden gebruikt.

Om burgers, bedrijven en instellingen meer privacybewust te maken zijn nieuwe meetmethoden vereist. Privacy is echter niet zozeer een hightech probleem, maar vooral een human probleem. Voor een hightech - human touch universiteit zoals de UT liggen hier dus legio kansen. Zo zijn er ethische vragen: weet de bezoeker van een website wel precies welke informatie wordt verzameld en wat er met deze informatie wordt gedaan? Wordt niet meer informatie verzameld dan strikt noodzakelijk is? Ook zijn er juridische vragen, zeker omdat bedrijven zoals Google buiten het bereik van de Nederlandse wetgever vallen.

De kern van het privacyprobleem is de schaal waarop data wordt verzameld. Vroeger wisten vele partijen ieder een klein beetje; er werd wel veel geroddeld maar een dorp verder wist bijna niemand meer wie je was. Tegenwoordig weten een klein aantal wereldwijd opererende bedrijven bijna alles over je. Hoe gezond je bent, of je wel op tijd gaat slapen, wie je vrienden zijn, wat je op TV bekijkt, of je stiekum denkt aan een nieuwe baan. Een zwangerschapstest is straks niet meer nodig, want of je zwanger bent kan je gewoon aan Google vragen.

4. DDoS-aanvallen

Een groot probleem voor de goede werking van het Internet en de daarop aangesloten systemen en diensten zijn zogeheten Distributed Denial of Service (DDoS) aanvallen. Bij een dergelijke aanval krijgt een systeem of Internetdienst zoveel verkeer te verwerken, dat het onder de last bezwijkt. Er zijn verschillende soorten aanvallen mogelijk. De aanvaller kan zich richten op één cruciaal element van de dienst, zoals het login-systeem van een bank, door geprepareerde berichten daarheen te sturen. Vaak ziet men echter een brute-force aanval op de verbinding tussen het Internet en de dienst. Er wordt dan zoveel verkeer gestuurd dat de Internetaansluiting wordt overbelast; de precieze inhoud van de berichten is dan onbelangrijk.

Begin 2014 had de tot nog toe grootste DDoS-aanval een kracht van 400 Gbps; op de UT hebben we recentelijk nog een aanval gehad van 20 Gbps. De UT en vergelijkbare universiteiten zijn sinds kort met 40 Gbps op SURFnet aangesloten en kunnen een aanval van 20 Gbps dus nog net verwerken. Banken, verzekeringsmaatschappijen en andere instellingen hebben echter vaak een aansluitcapaciteit van 1 Gbps of minder, en zijn dus veel kwetsbaarder.

Als een aanval op een groot bedrijf een paar uur duurt, kan de schade snel oplopen tot enige miljoenen euros. Er zijn vermoedens dat criminele partijen regelmatig korte aanvallen uitvoeren op de meest populaire websites (de Alexa 500), om te testen of de infrastructuur bestand is tegen dergelijke aanvallen. Indien men niet bestand is, krijgt men een voorstel van de criminele organisatie om verdere aanvallen af te kopen. Dergelijke maffiose praktijken komen echter beperkt in het nieuws, mede omdat slachtoffers reputatieschade willen vermijden en andere criminelen niet op verkeerde gedachten willen brengen.

Niet alle DDoS-aanvallen worden uitgevoerd door criminele organisaties. Sinds het najaar van 2012 zien we dat ook scholen en ROCs worden aangevallen. Als we het patroon van de aanval leggen naast het proefwerk- of tentamenrooster, dan

is vaak meteen duidelijk dat één van de scholieren voor de aanval verantwoordelijk is. Vaak gaat het om jongens van een jaar of 16, die thuis op hun zolderkamer achter de computer Internetgames spelen; ik gebruik voor het gemak de term script-kiddies voor dergelijke jongeren. In de wereld van Internetgames is in principe alles toegestaan; als je tegenstander aan de winnende hand is, dan DDoS je hem gewoon van het net. Hoewel ik hiervoor geen bewijzen heb, vermoed ik dat een deel van de aanvallen op banken door script-kiddies wordt uitgevoerd, die graag het 8 uur journaal willen halen. Vroeger waarschuwden de media bij langdurige droogte voor het gevaar van bos- en heidebranden; sinds deze waarschuwingen niet meer worden verspreid is het aantal bos- en heidebranden afgenomen. Misschien dat het journaal ook minder tijd aan DDoS-aanvallen zou moeten besteden.

In de wetenschappelijke wereld is al lang bekend hoe DDoS-aanvallen eruit zien; de techniek achter DDoS-aanvallen leggen we bijvoorbeeld al tien jaar uit in ons vak Network Security. Bij het grote publiek raakten deze aanvallen echter pas bekend in 2010, toen een groep sympathisanten van wikileaks onder de naam 'Anonymous' op grote schaal aanvallen ging uitvoeren op websites van creditcardmaatschappijen [19]. Het uitvoeren van dergelijke aanvallen bleek kinderlijk eenvoudig, omdat slechts een tool met de naam LOIC (Low Orbit Ion Cannon) geïnstalleerd hoefde te worden. Korte tijd later werd het uitvoeren van DDoS-aanvallen nog eenvoudiger, omdat een aantal websites 'DDoS as a Service' gingen aanbieden. Na betaling van een paar euro kan iedere script-kiddie via deze websites aanvallen uitvoeren op een willekeurig doel. Deze 'diensten', die ook wel bekend staan onder de namen 'booter' en 'stresser', blijken uiterst effectief te zijn.

4.1. Hoe werkt een DDoS-aanval

Bij een DDoS-aanval wordt zoveel Internetverkeer naar een bepaald doelwit gestuurd, dat deze onder de last bezwijkt. Om de identiteit van de echte aanvaller te versluieren, worden aanvallen vaak uitgevoerd via een derde partij. Deze derde partij is meestal een Internetserver die diensten aanbied via het UDP-protocol. Voorbeelden van dergelijke diensten zijn het

Domain Name System (DNS), het Network Time Protocol (NTP), CharGen, en het Simple Network Management Protocol (SNMP).

Omdat er gebruik wordt gemaakt van een derde partij, worden dergelijke aanvallen aangeduid met de term 'reflection'. Reflection werkt, omdat de UDP-server het IP-adres van de zender niet kan controleren. Als een aanvaller in het source-adres van een UDP-bericht het IP-adres zet van het systeem dat moeten worden aangevallen, dan zal de UDP-server het antwoord naar dit adres sturen. Deze techniek heet IP-Spoofing, en is te vergelijken met het zetten van een vals adres onder een brief; de ontvanger zal eventuele antwoorden dan terugsturen naar dit valse adres.

Een tweede techniek die gebruikt wordt is amplification, of in goed Nederlands 'versterking'. Deze techniek maakt gebruik van het feit dat een antwoord vaak veel groter is dan de oorspronkelijke aanvraag. Dit effect is vergelijkbaar met het sturen van een kaartje naar Ikea, met het verzoek de catalogus terug te sturen. De aanvraag past op 1 pagina, maar de catalogus heeft maar liefst 326 pagina's. De versterkingsfactor is dus 326. Bij een aantal UDP-gebaseerde diensten is een versterkingsfactor van 100 in specifieke gevallen goed haalbaar; als de aanvaller met 100 Mbps pakketjes stuurt naar een DNS-server, dan zal de DNS-server 10 Gbps versturen naar het slachtoffer.

Figuur 4.1 toont de resultaten van een recente studie die door ons is verricht om de versterkingsfactor van DNS te bepalen [20]. DNS is een cruciale component binnen het Internet omdat het domeinnamen, zoals `www.utwente.nl` vertaalt in IP-adressen zoals `130.89.3.249`. De figuur laat zien dat bij normale DNS (authoritative) systemen de versterkingsfactor gemiddeld ligt bij ongeveer 6; in geval van DNSSEC, dus de 'veilige versie' van DNS, ligt deze waarde net onder de 50. Het verschil tussen DNS en DNSSEC kan worden verklaard door het feit dat bij DNSSEC digitale handtekeningen worden meegestuurd, om de correctheid van het antwoord te kunnen verifiëren. DNSSEC is dus een stuk veiliger dan DNS, maar deze verhoogde veiligheid zorgt wel voor een verhoogde gevoeligheid voor DDoS-aanvallen. Door gerichte maatregelen te

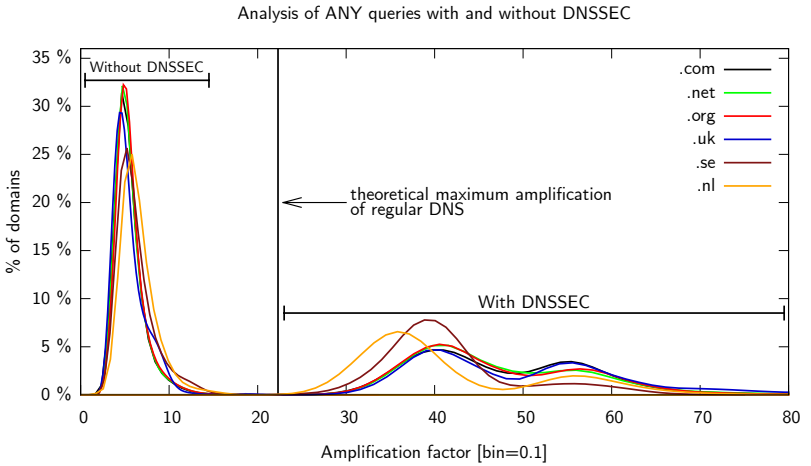

Fig. 4.1: DNS versterkingsfactor

nemen, zoals verificatie van het IP-adres van de aanvrager, of door het antwoord te beperken tot een deel van de gevraagde informatie, is het gelukkig wel mogelijk deze gevoeligheid te verminderen. Ook moet opgemerkt worden dat DNS-amplification aanvallen vaak gebruik maken van speciaal geprepareerde 'open resolvers' in plaats van de authoritative servers die bij bovenstaande metingen zijn gebruikt. De versterkingsfactor die mogelijk is bij dergelijke open resolvers is veel groter dan de factor 6 van bovenstaande metingen.

Tenslotte zal een aanvaller zich niet beperken tot een enkele UDP-server, maar de aanval distribueren over honderden of zelfs duizenden UDP-servers. Het voordeel van gedistribueerde aanvallen is dat ze veel lastiger te bestrijden zijn. Als IKEA opeens gevraagd wordt honderden catalogi naar eenzelfde adres te sturen, dan zal dit worden opgemerkt waarna verzending stopt. Als echter de aanvaller één enkele catalogus bij IKEA opvraagt en daarnaast catalogi bij honderden andere bedrijven, dan zal de aanval niet eenvoudig voortijdig gedetecteerd en gestopt kunnen worden.

Voor de aanval die begin dit jaar een kracht had van 400 Gbps, zijn ruim 4500 NTP-servers misbruikt, verspreid over bijna 1300 netwerken. Bij een aanval verleden jaar op de

Spamhaus-infrastructuur werden zelfs meer dan 30 duizend open DNS-Resolvers misbruikt, alhoewel die aanval 'slechts' een kracht had van 300 Gbps [21].

4.2. DDoS as a Service

De DDoS-aanvallen op scholen die sinds enige jaren worden uitgevoerd maken in het algemeen gebruik van de eerder genoemde 'booters', dus websites waar men voor een betaling van een paar euro een echte DDoS-aanval kan uitvoeren. Om een indruk te krijgen hoe effectief deze 'DDoS as a Service' diensten zijn hebben we een jaar geleden een serie aanvallen uitgevoerd op onze eigen systemen [22]. Voordat we met deze aanvallen zijn begonnen hebben we uiteraard eerst met de netwerkbeheerders van de UT en SURFnet overleg gehad, om zeker te stellen dat er door deze aanvallen geen onvoorziene schade zou worden aangericht. Voor de veel grotere DDoS-metingen die we binnenkort als onderdeel van het nieuwe NWO D3 cybersecurity project gaan verrichten hebben we sinds kort ook toestemming van het openbaar ministerie.

Van de 14 geteste booters bleken er 9 'bruikbaar' voor een daadwerkelijke aanval. De kosten voor een abonnement bij deze booters varieert tussen de 1,95 euro en 10,90 euro; betaald wordt via Paypal. Een abonnement is één tot meerdere maanden geldig en in deze periode kunnen net zoveel aanvallen uitgevoerd worden als gewenst.

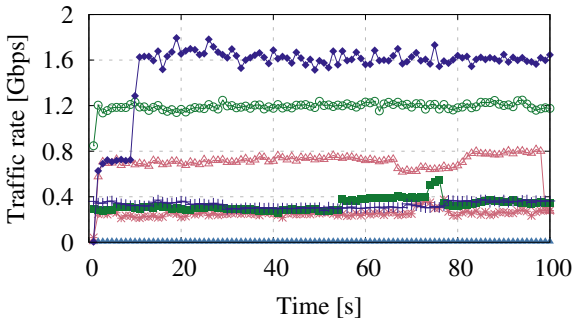

Fig. 4.2: Hoeveelheid verkeer bij een DNS gebaseerde DDoS-aanval

Figuur 4.2 toont de hoeveel verkeer die per booter wordt gegenereerd bij een gedistribueerde DNS-reflection aanval. De figuur laat zien dat de meeste booters met gemak enige honderden Mbps kunnen genereren; een enkel booter haalt zelfs 1,6 Gbps.

Naast DNS werden ook andere UDP-gebaseerde diensten misbruikt voor DDoS-aanvallen. Een interessant voorbeeld wordt getoond in figuur 4.3; dat de hoeveelheid verkeer bij CharGen-gebaseerde aanvallen laat zien. CharGen is een uiterst eenvoudig testprotocol, dat nog uit de begintijd van het Internet stamt en in veel systemen is ingebouwd. Uit de figuur blijkt dat de sterkste aanval (door booter 9) een piek heeft bereikt van ongeveer 7 Gbps.

Scholen, maar ook veel andere instellingen, kunnen met gemak door aanvallen van deze grootte van het Internet worden afgesneden. Een vraag die opkomt is of het mogelijk zou zijn aanvallen verder te versterken door alle booters gelijktijdig te gebruiken. Uit figuur 4.4 blijkt dat er weinig overlap is tussen de systemen die de verschillende booters inzetten voor hun DNS- en CharGen-gebaseerde reflection-aanvallen. Alleen tussen booter 6 en 7 is er een sterke correlatie: ruim 98 % van de door booter 6 gebruikte open DNS-resolvers worden ook gebruikt door booter 7. Verder blijkt dat de door booter 5 gebruikte open DNS-resolvers voor ongeveer 10% samenvallen met de systemen die booters 6 en 7 gebruiken. In het merendeel van de gevallen maken booters echter gebruik van verschillende systemen voor hun reflection-aanvallen; we mogen dus aannemen dat bij een gelijktijdige aanval van alle booters

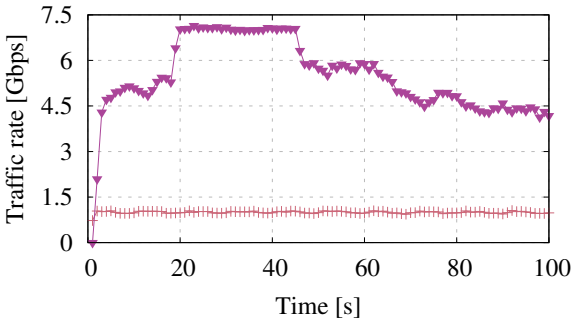

Fig. 4.3: Hoeveelheid verkeer bij een CharGen gebaseerde DDoS-aanval

∩	B1	B2	B3	B4	B5	B6	B7	B8	B9
B1	–	0.20	0.20	3.88	0.02	1.07	0.73	0	0
B2	11.54	–	0	0	0	0	0	0	0
B3	16.67	0	–	0	0	1.85	1.85	0	0
B4	5.86	0	0	–	0.20	4.11	1.04	0	0
B5	0.01	0	0	0.07	–	8.38	7.99	0	0.08
B6	0.65	0	0.01	1.65	9.42	–	81.33	0	0.07
B7	0.54	0	0.02	0.51	10.90	98.65	–	0	0.08
B8	0	0	0	0	0	0	0	–	43.06
B9	0	0	0	0	0.18	0.13	0.13	3.20	–

Fig. 4.4: Overlap tussen de 'infrastructuur' van de verschillende booters

op hetzelfde doelwit veel meer verkeer wordt gegenereerd dan bij een aanval door een enkele booter.

In potentie zouden booters nog veel sterkere aanvallen kunnen uitvoeren. Uit recente studies blijkt dat er wereldwijd minimaal 89000 CharGen-servers beschikbaar zijn [23]. Bij onze metingen gebruikte booter 9 'slechts' 3779 CharGen servers; indien booter 9 alle beschikbare CharGen-servers had ingezet, zouden aanvallen bijna 25 keer sterker zijn uitgevallen, dus een kracht hebben gehad tussen de 150 en 200 Gbps. Nog dramatischer wordt de situatie als een aanvaller alle open DNS-resolvers zou weten in te zetten. Recente metingen schatten het aantal open DNS-resolvers op ongeveer 25 miljoen; dit aantal is ruim 3000 keer groter dan wat wij bij de aanvallen op onze eigen infrastructuur hebben gemeten [24]. Aanvallen met een kracht van meerdere Tbps zijn dus relatief eenvoudig realiseerbaar.

De conclusie die we kunnen trekken is dat iedereen die een webbrowser kan bedienen en beschikking heeft over een Paypal account aanvallen kan verrichten met een kracht die voldoende is om veel bedrijven en instellingen van het Internet te halen. Indien booters hun aanvallen zouden willen versterken, of indien iemand met iets meer verstand van het Internet kwaad zou willen doen, is het vrij eenvoudig aanvallen te lanceren die factoren sterker zijn dan alles wat we tot nu toe hebben gezien. De grote aanval van 400 Gbps eerder dit jaar is dus nog maar het topje van de ijsberg.

4.3. DDoS Protection Services

De vraag die men zich moet stellen is hoe bedrijven en instellingen zich kunnen beschermen tegen DDoS-aanvallen. De eerste stap die een potentieel doelwit uiteraard moet nemen, is de capaciteit van de verbindingen met het Internet ruim te dimensioneren, en voor een goede firewall te zorgen. Helaas zal deze stap in een aantal gevallen onvoldoende blijken te zijn. Bedrijven en instellingen kiezen daarom vaak voor diensten van zogeheten DDoS protection services, zoals Cloudflare, Incapsula en Prolexic. Deze bedrijven herrouteren al het Internetverkeer van hun klanten zodat het door speciale filters bewerkt kan worden die het aanvalsverkeer verwijderen. Deze filterdiensten worden ook wel aangeduid als 'wasmachine' of 'wasstraat'. Om zelf niet overbelast te raken wordt het 'wassen' van het Internetverkeer gelijktijdig op meerdere locaties uitgevoerd. Het verkeer van de bedrijven die van deze 'gedistribueerde wasdienst' gebruik maken wordt daarom op meerdere plaatsen van het normale Internet afgetakt, liefst zo dicht mogelijk bij de aanvalsbron. Om verkeer te herrouteren, wordt gebruik gemaakt van BGP of DNS.

Het gebruik van DDoS protection services heeft ook nadelen. Gebruikers moeten meestal voor deze diensten betalen, zodat niet-commerciële partijen hiervan vaak geen gebruik kunnen maken. Belangrijker is echter dat alle huidige DDoS protection services worden aangeboden door Amerikaanse bedrijven, zodat de NSA op legale wijze toegang krijgt tot de inhoud van al het Internetverkeer. Alhoewel ook op dit moment de NSA reeds op grote schaal Internetverkeer onderschept, is het probleem dat DDoS protection services ook de sleutels bezitten om het encrypted (HTTPS) verkeer te kunnen decoderen en 'wassen'. Door gebruik te maken van DDoS protection services krijgt de NSA dus ook toegang tot verkeer dat met behulp van versleuteling beveiligd is. Instellingen die gevoelige informatie verwerken, zoals de belastingdienst, banken en verzekeringsmaatschappijen, kunnen dus beter geen gebruik maken van Amerikaanse DDoS protection services.

Een interessant fenomeen is dat booters, dus websites die DDoS-aanvallen als dienst aanbieden, zich zelf vaak weer

beschermen tegen aanvallen van concurrenten door ook van DDoS protection services gebruik te maken. DDoS protection services kunnen in principe dus precies volgen welke aanvallen worden besteld en kunnen voordat de aanval begint alvast maatregelen treffen. Bovendien kan de persoon die de aanvallen heeft besteld ook getraceerd worden, omdat het gebruikte Paypal account bekend is. Overigens zijn er ook sterke aanwijzingen dat sommige booters samenwerken met de FBI. Scholieren die via Booters hun school willen aanvallen zijn dus gewaarschuwd.

4.4. Hoe verder

Bij veel DDoS-aanvallen wordt gebruik gemaakt van reflection via DNS, NTP, CharGen en andere UDP-gebaseerde servers. Zoals al is uitgelegd in sectie 4.1, wordt bij reflection gebruik gemaakt van IP-Spoofing, wat wil zeggen dat het IP-adres van de bron vervangen is door het adres van het slachtoffer. Het is relatief eenvoudig IP-Spoofing te bestrijden; Internet access providers hoeven slechts te controleren of het gebruikte bron adres wel door hen is uitgegeven. Reeds in het jaar 2000 heeft de IETF een document gepubliceerd met de titel: 'Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing'; dit document staat bekend onder de naam 'Best Current Practices 38' (BCP38) [25]. Helaas wordt deze aanbeveling nog niet door alle providers geïmplementeerd. Zoals ons eerdere onderzoek naar Internet Bad neighborhoods reeds liet zien lijkt het erop dat niet alle providers belang hebben bij een veilig Internet. Internationale wetgeving op dit gebied lijkt dan ook wenselijk. Helaas lijkt het aantal politici en juristen met verstand van ICT relatief klein, zodat uit deze hoek voorlopig weinig steun valt te verwachten.

Aan de UT gaan we, samen met partijen zoals SURFNet en Logius, in het kader van ons nieuwe NWO 'Distributed Denial of Service Defense' (D3) project werken aan nieuwe technieken om DDoS-aanvallen te detecteren en bestrijden. Daarbij zullen de mogelijkheden van nieuwe ontwikkelingen, zoals 'Software Defined Networking' (SDN) en 'OpenFlow', bestudeerd worden om concepten zoals 'Firewall as a Service' te realiseren.

5. De veranderende universiteit

In het voorgaande ben ik uitgebreid ingegaan op de veranderingen die op mijn vakgebied plaatsvinden. Ook de universiteit is echter continu in verandering. Aan deze veranderingen wil ik een paar woorden weiden.

5.1. Onderwijs

Binnen een universiteit zijn onderwijs en onderzoek even belangrijk. Graag wil ik daarom ook iets zeggen over de gevolgen van het Internet voor het universitaire onderwijs.

In het verleden lag het kennismonopolie bij de docent. Als de docent iets beweerde dan was dat waar. Studenten hadden nauwelijks mogelijkheden de docent te controleren, laat staan te corrigeren.

In de jaren vijftig schreef een docent alles op het bord en moesten de studenten eigen aantekeningen bijhouden van alles wat door de docent werd gezegd en geschreven. In de jaren zeventig waren een aantal docenten zo vriendelijk om hun notities te bundelen in een dictaat; de studenten hoefden nu niet meer alles van het bord over te schrijven. Weer twintig jaar later werden de beste dictaten als boek uitgegeven; een docent hoefde nu niet meer zelf een dictaat te maken, maar kon een boek van elders gebruiken. Ondertussen is het bord vervangen door powerpoint-slides, die vaak gebaseerd zijn op slides die de uitgever van het boek heeft meegeleverd danwel elders op het Internet te vinden zijn. Als tijdens college iets onduidelijk blijft, dan zoeken studenten onmiddellijk via hun notebook of iPad een nadere uitleg op Wikipedia.

Omdat informatie nu overal via het Internet is te vinden, is de rol van de docent veranderd. In plaats van het *creëren* van informatie ligt de nadruk op het *selecteren* van informatie, en het begeleiden van studenten.

De informatie die docenten momenteel op het Internet vinden is nog vaak statisch van aard: e-books, powerpoint-slides en wikipedia. Daarin komt echter snel verandering. Op YouTube

en vergelijkbare sites kan men steeds vaker korte video's vinden die op een een uitstekende wijze een bepaald onderwerp behandelen. Een traditioneel hoorcollege gegeven door een conservatieve docent kan met geen mogelijkheid het beter doen dan een dergelijke video. Ook kunnen studenten steeds vaker via het Internet interactieve opdrachten uitvoeren; in mijn vakken maak ik al graag gebruik van deze mogelijkheid. Soms gebruik ik materiaal en opdrachten die ontwikkeld zijn door anderen, maar zelf ben ik ook actief met het ontwikkelen van onderwijsvideo's en web-based opdrachten. Een universitair medewerker moet niet alleen de ambitie hebben op onderzoeksgebied veel geciteerd te worden, maar moet ook wereldwijd bekend willen worden met specifieke onderwijs video's en opdrachten. Wat is leuker: 100 citaties op een artikel of 10.000 studenten die een stukje van je onderwijs volgen?

5.2. Onderzoeksfinanciering

Toen ik in 1983 als onderzoeker aan deze universiteit mijn carrière begon, werden alle onderzoekers rechtstreeks betaald vanuit de universiteit (de 1st geldstroom). De vakgroep IPS, waarvan ik toen lid was, had grootse plannen en veel ambitie, en wilde meedoen aan een extern project dat in het kader van het ESPRIT-programma door de EU zou worden gefinancierd. Dit plan viel echter niet in goede aarde bij een deel van de faculteit; als externe partijen zoals de EU voor ons onderzoek zouden gaan betalen, dan zouden ze de keuze van onze onderzoeksthema's beïnvloeden, waardoor onze wetenschappelijke onafhankelijkheid in gevaar zou komen. Na een verhit debat in de faculteitsraad, waarbij we door het CvB werden gesteund, mochten we uiteindelijk toch aan het extern gefinancierde project meedoen.

Hoe tijden kunnen veranderen. Bij onze vakgroep DACS worden op dit moment 6 personen rechtstreeks betaald vanuit de universiteit en 19 personen vanuit externe projecten. Omdat deze zes personen naast onderzoek ook verantwoordelijk zijn voor de financiering van het onderwijs, het secretariaat en het management, wordt momenteel meer dan 80% van ons onderzoek extern gefinancierd.

De verschuiving richting extern gefinancierd onderzoek zorgt er voor dat er steeds minder personeel is met een vaste aanstelling en dat vooral jongeren alleen nog maar tijdelijk contracten krijgen. Binnen onze DACS-groep hebben van de 25 medewerkers slecht 6 een vaste baan. Men kan beargumenteren dat een deel van de tijdelijke medewerkers als AIO en dus op een opleidingsplaats is aangesteld en daarom geen vaste positie hoeft te hebben. Daarnaast is er echter wel een groeiende groep gepromoveerde medewerkers waarvoor ook geen vaste positie meer beschikbaar is, de zogeheten Post-Docs. Deze groep medewerkers wordt steeds vaker ingezet voor onderwijs, het managen van projecten en de dagelijkse begeleiding van promovendi; zonder PostDocs zouden veel onderzoeksgroepen niet goed meer kunnen functioneren. Ik ben dan ook van mening dat er meer aandacht en rechtszekerheid moet komen voor deze groeiende groep jonge onderzoekers.

Het feit dat het merendeel van ons onderzoek verricht wordt door tijdelijk personeel heeft alles te maken met geld. In het jaar 2000 hebben Europese landen in Lissabon afgesproken 3% van hun Bruto Binnenlands Product (BBP) aan research en development (R&D) te besteden. Europa moest veranderen in de meest concurrerende en dynamische kenniseconomie van de wereld. Deze doelstelling is duidelijk niet gehaald; we blijken in Nederland minder dan 2% van ons BBP te investeren in R&D, en verliezen ten opzichten van de overige Europese landen duidelijk terrein [26].

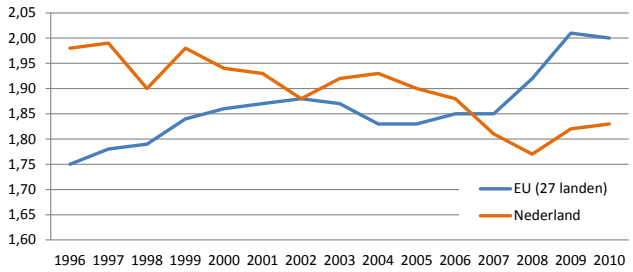

Fig 5.1: Investeringen in R&D in % van BBP (bron: VSNU [26])

Zo wordt er sinds 2011 door de overheid vanuit het Fonds Economische Structuurversterking (FES) geen geld meer geïnvesteerd in de Nederlandse kenniseconomie. Wel heeft de overheid een zogeheten 'topsectoren beleid' ontwikkeld, maar dit beleid leidt tot veel minder promovendi dan bij eerdere programma's zoals COMMIT en BSIK. Initieel is er wel geïnvesteerd in het bedenken van plannen en het formeren van netwerken, maar ik zie, behalve binnen het NWO cyber security programma, geen geld voor promovendi. In totaal is er voor het cyber security programma in Nederland 12,7 miljoen euro beschikbaar (de overheid betaald hiervan 43%, NWO de rest). Ter vergelijking: wij werken veel samen met onderzoekers in München en Darmstadt. In Beieren is er voor het 'Sicherheitscluster München' 30 miljoen euro beschikbaar, en eenzelfde bedrag heeft de deelstaat Hessen beschikbaar gesteld voor het 'Center for Advanced Security Research Darmstadt' (CASED). Ten opzichte van de buitenlandse competitie lopen we dus ook op het gebied cyber security achter.

5.3. Publiceren en Open Access

In 1980 bestond de totale wetenschappelijke output van de toenmalige *vakgroep* Informatica uit één promotie, twee journal artikelen, een handjevol conferentiebijdragen en nog wat interne memoranda [27]. Op dit moment wordt een dergelijke output gemakkelijk door een enkele wetenschapper gehaald. Dat is op zich goed nieuws. Maar de focus op Key Performance Indicatoren (KPI), met name publicaties, citaties en H-indices, lijkt af en toe ook wel wat door te slaan; niet alleen in Twente, maar ook elders in de wereld.

Alles waarvoor geen KPI is vastgelegd verdwijnt. Onze groep heeft altijd veel aan de ontwikkeling van internationale standaarden bijgedragen, maar voor dergelijke activiteiten is, zeker na een aantal reorganisaties, geen plaats meer. Het gebrek aan geld en vaste posities heeft ervoor gezorgd dat er een sterke competitie is ontstaan; het is veel meer dan vroeger "ieder voor zich" geworden. PostDocs moeten vechten om ergens in de wereld een vaste positie of tenure track te krijgen. Ze moeten strategisch opereren, en dus vooral aan hun eigen H-index denken.

Waar we ons nog te weinig zorgen over maken, is dat de druk om te publiceren (publish or perish) tot uitwassen kan leiden. KPIs zoals een H-index zijn gemakkelijk te manipuleren. Er is een hele nieuwe business ontstaan rond de organisatie van conferenties. Er zijn genoeg voorbeelden van fancy conferenties, waarbij de organisatoren veel geld verdienen, maar geen serieus reviewproces organiseren. Open access tijdschriften schieten als paddestoelen uit de grond, maar zijn soms primair opgericht om snel geld mee te verdienen. Auteurs moeten immers voor iedere publicatie betalen, en er zijn nog teveel universiteiten wereldwijd waar een AIO pas mag promoveren als hij één of meerdere journal publicaties heeft.

Kwaliteitsbewaking wordt dus steeds belangrijker binnen de wetenschappelijke wereld. Volgens wikipedia gelden “voor het bewaken van wetenschappelijk onderzoek een aantal normen, die voor een deel ethisch van aard zijn. Deze normen worden in principe gehandhaafd via onderlinge controle, waarbij wetenschappers de resultaten van hun collega's beoordelen. De wetenschappelijke gemeenschap controleert dus zichzelf; de zogenaamde collegiale toetsing” [28]. Op het gebied van ICT-onderzoek wordt kwaliteitsbewaking gecoördineerd binnen drie professionele organisaties: ACM, IEEE en IFIP. Deze drie organisaties verzorgen ook de belangrijkste conferenties en tijdschriften op ons vakgebied en bewaken de kwaliteit van het reviewproces. Vanwege het belang dat ik hecht aan deze organisaties, draag ik hieraan ook graag bij, o.a. als (associate) editor van een aantal tijdschriften en als lid van de stuurcommissies van de meeste conferenties op mijn vakgebied (network operations and management).

Naast kwaliteit ligt de nadruk ook steeds vaker op vrije toegankelijkheid van wetenschappelijke publicaties. Organisaties zoals de EU en de VSNU propageren het publiceren in open access tijdschriften. Helaas zijn de consequenties waar onderzoekers bij open access tegenaanlopen niet altijd goed doordacht. Uitgevers van wetenschappelijke tijdschriften, zoals Elsevier, Springer en Wiley, zien hun businessmodel in gevaar komen. Professionele organisaties zoals ACM en IEEE zijn bang dat hun inkomsten uit tijdschriften en Digital Libraries teruglopen. Omdat ze echter wel begrijpen dat open access

een steeds grotere rol gaat spelen, geven ze toch de mogelijkheid artikelen als open access te publiceren. Ze vragen echter per artikel bedragen tussen $500 en $3000; bedragen die in geen enkele verhouding staan met de werkelijke kosten. Bijna al het werk wordt immers al gedaan door de auteurs (de meeste artikelen worden camera-ready aangeleverd) en reviewers, die niet betaald worden maar op vrijwillige basis werken. De bedragen van $500 tot $3000 lijken te zijn ingegeven door de wens om een oud businessmodel te handhaven. De kosten worden neergelegd bij onderzoeksgroepen die veel publiceren. Bijvoorbeeld: als onze vakgroep DACS alleen nog maar 'open access' zou publiceren, zouden we hiervoor 5 tot 10% van ons onderzoeksbudget moeten gebruiken, en dus 5 tot 10% van onze onderzoekers moeten ontslaan. Het zal duidelijk zijn dit niet de bedoeling is van organisaties zoals de EU en VSNU.

Een essentiële rol is volgens mij weggelegd voor professionele organisaties die wel reputatie, maar geen businessmodel te verliezen hebben. Een voorbeeld van een dergelijke organisatie op mijn vakgebied is de 'International Federation for Information Processing' (IFIP), die opgericht is onder auspiciën van de UNESCO. IFIP heeft een kleine staf en publicaties daarom in het algemeen uitbesteed bij Springer (als onderdeel van de LNCS of AICT series). Ondanks het feit dat Springer zorg draagt voor de proceedings van IFIP-conferenties, blijft het copyright bij IFIP. Hierdoor is het mogelijk om publicaties als open access uit te geven, zonder dat de auteurs hiervoor moeten betalen. De echte kosten van open access, een paar euro per publicatie, betaald IFIP wel uit andere middelen.

Als voorzitter van IFIP TC6 (Communication Systems) en als lid van IFIP's publication committee heb ik me dan ook sterk gemaakt voor de implementatie van IFIP's open digital library (DL). Geïnitieerd vanuit TC6 en gesponsord door ons EU 'Network of Excellence' project Flamingo, hebben we een initiële versie van IFIP's open DL opgezet die nu draait op één van onze UT-machines [29]. Het plan is op termijn IFIP's open DL te migreren naar het HAL systeem van INRIA, zodat professionele ondersteuning ook na afloop van ons EU-project gegarandeerd blijft.

6. Conclusie

Ik ben aan het eind van mijn betoog gekomen. Wat moet u van mijn verhaal onthouden?

Ten eerste dat een veilig Internet van cruciaal belang is voor onze samenleving. De uitdagingen zijn immens, en onderzoek is nodig op academisch niveau. Ik ben dan ook blij dat de UT op het gebied van '*network security*' een vooraanstaande rol kan spelen. Ons onderzoek vereist een multidisciplinaire aanpak, en past dus uitstekend binnen een universiteit die High-Tech - Human Touch als motto heeft. Onze groep werkt dan ook samen met bijvoorbeeld ethici uit de groep van Philip Brey en Peter-Paul Verbeek, alsmede bedrijfskundigen uit de groep van Jos van Hillegersberg en Bart Nieuwenhuis.

Ten tweede moet u onthouden dat ook veiligheidsdiensten een bedreiging vormen voor de veiligheid op het Internet. In plaats van veiligheidsgaten te dichten, worden gaten geëxploiteerd en soms zelfs gecreëerd. Een aantal westerse veiligheidsdiensten bouwt eigen botnets, met het doel daarmee op grote schaal in te breken. Ik pleit er voor dat overheden per wet verbieden dat veiligheidsdiensten *onbeperkt* gegevens verzamelen over *alle* op het Internet aangesloten systemen en dat ze zonder *rechterlijke goedkeuring* niet op willekeurige Internetsystemen mogen inbreken. Veiligheidsdiensten moeten *verplicht* worden eventueel door hen gevonden veiligheidsproblemen te melden.

Ten derde dat burgers, bedrijven en instellingen nog naïef en weinig privacybewust zijn. Ogenschijnlijk onschuldige informatie, zoals surfgedrag en lijstjes met vrienden, wordt nu al door commerciële bedrijven 'gebruikt' om te bepalen of iemand een verzekering of hypotheek kan krijgen.

Ten vierde moet u onthouden dat script-kiddies al voor een paar euro een DDoS-aanval kunnen uitvoeren met voldoende kracht om de meeste bedrijven en instellingen van het Internet te verwijderen. Verder onderzoek is dringend nodig om de detectie en bestrijding van dergelijke DDoS-aanvallen effectiever te maken.

7. Tenslotte

Ik zou willen afsluiten met het bedanken van die personen zonder wie ik hier vandaag niet zou hebben gestaan. In eerste instantie is dat mijn afstudeerhoogleraar en promotor Chris Vissers, aan wie ik ook in de periode dat Chris al lang bij het Telematica Instituut zat veel te danken heb. Ook wil ik Kees Bakker, mijn co-promotor, en Ignas Niemegeers, mijn latere leidinggevende, bedanken voor de vele goede adviezen en inzichten, van Ignas heb ik bovendien geleerd dat een hoogleraar ook een fascinatie voor de nieuwste technische snufjes op HIFI gebied kan hebben. Vervolgens wil ik Boudewijn Haverkort bedanken, niet alleen voor je enthousiasme waarmee je altijd probeert de vakgroep en de universiteit vooruit te helpen, maar zeker ook voor de onvoorwaardelijke steun en de altijd fijne samenwerking en gesprekken.

Ton Mouthaan, de toenmalige decaan, Peter Apers, de toenmalige directeur van het CTIT, en Ed Brinksma, de huidige rector, wil ik bedanken voor mijn benoeming en het in mij gestelde vertrouwen.

Onze groep met het thema 'Network Operations and Management' heeft de laatste jaren een geweldige ontwikkeling doorgemaakt van traditioneel network management richting network measurements met een focus op network security. Deze ontwikkeling was nooit mogelijk geweest zonder de fantastische ondersteuning van mijn PostDocs en AIOs. Wat ik bijzonder waardeer is dat we een echte groep zijn geworden en samen veel verder zijn gekomen dan wanneer ieder voor zich zou zijn gegaan. Daarnaast hebben we met elkaar veel plezier, iets waar ik echt van geniet. Ik wil bij deze gelegenheid dan ook al mijn PostDocs en AIOs bedanken: Ramin, Anna, Robert, Remco, Tiago, Giovane, Idilio, Rafael, Ricardo, Rick, Jair, Morteza, Jessica, Roland, Luuk, Christian en Mattijs.

Ik ben heel blij dat ik me precies 10 jaar geleden kon aansluiten bij de vakgroep DACS. Niet alleen heb ik hierdoor mijn onderzoek kunnen invullen op de manier die mij voorstond, maar ook heb ik een aantal geweldige collegae

gevonden. Ik wil Jeanette, Geert, Pieter-Tjerk, Anne, Georgios en alle anderen hartelijk danken.

Alhoewel een dag als vandaag toch vooral in het teken staat van onderzoek en activiteiten binnen deze universiteit, besef ik heel goed dat familie en vrienden nog veel belangrijker zijn dan een benoeming tot hoogleraar. Ik wil daarom mijn moeder, Betty, Marry, Anke, Bert, Hans, Josien, Joost, Marjolijn, Liseth en Stefan bedanken voor alle gezelligheid en steun, ook in tijden waarin het wel eens tegen zat. Tenslotte is er één persoon die meer mooie woorden verdient dan ik als bèta kan bedenken. Daarom houd ik het kort: Wilma, ik hoop dat we nog lang samen van het leven kunnen genieten.

Ik heb gezegd.

Referenties[1]

[1] Blaauw, G.A. (1980): *Dictaat Computer Architectuur*, Sectie 1.1, Universiteit Twente

[2] Hofstede, R. et al (2014): *Flow Monitoring Explained: From Packet Capture to Data Analysis with NetFlow and IPFIX*, IEEE Communication Surveys and Tutorials

[3] Steinberger, J. et al (2013): *Anomaly Detection and mitigation at Internet scale: A survey*, Proceedings of the 7th International Conference on Autonomous Infrastructure, Management and Security, AIMS'13, LNCS, vol. 7943, pp. 49–60.

[4] Opstelten, I.W. (13-8-2014): *Beantwoording Kamervragen over het bericht dat cybercrime Nederland jaarlijks 8,8 miljard euro kost*
http://www.rijksoverheid.nl/onderwerpen/cybercrime/documenten-en-publicaties/kamerstukken/2014/08/15/antwoorden-kamervragen-over-bericht-dat-cybercrime-nederland-jaarlijks-8-8-miljard-euro-kost.html

[5] Heise (15-8-2014): NSA/GCHQ: *The HACIENDA Program for Internet Colonization*, Vol. 2014/19, pag. 26
http://www.heise.de/ct/artikel/NSA-GCHQ-The-HACIENDA-Program-for-Internet-Colonization-2292681.html

[6] Durumeric, A. et al (2014): *The Matter of Heartbleed*, Proceedings of the 14th ACM Internet Measurements Conference, IMC'14

[7] Bloomberg (12-4-2014): *NSA Said to Exploit Heartbleed Bug for Intelligence for Years*
http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html

[8] eWeek (19-4-2014: *Heartbleed SSL Flaw's True Cost Will Take Time to Tally*
www.eweek.com/security/heartbleed-ssl-flaws-true-cost-will-take-time-to-tally.html

[9] Chaos Computer Club (26-10-2011): *Chaos Computer Club analysiert aktuelle Version des Staatstrojaners*
http://ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner

[10] NY Times (5-9-2013): *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*
http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

[11] IFIP statement on intentional weakening of security and trust mechanisms in ICT and the Internet by government agencies and other major actors

[1] *Alle URLs zijn gecontroleerd op 20-10-2014*

http://www.ifip.org/images/stories/ifip/public/Announcements/web%20ifip%20statement%20underminingsecuritytrust%20mechanisms%204%200.pdf
[12] The Guardian (8-6-2013): *NSA's Prism surveillance program: how it works and what it can do*
http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google
[13] The Intercept (12-3-2014): *How the NSA plans to infect 'Millions' of computers with malware*
https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/
[14] von Clausewitz, C (1832): *Vom Kriege, Über die Natur des Krieges*, 11. Aufl., S. 640
http://www.clausewitz.com/readings/Compare/VomKriege1832/Book1Ch01VK.htm
[15] Auke van der Woud (2006): *Een nieuwe wereld - Het ontstaan van het moderne Nederland*, pag. 343 & 348.
[16] Zetter, K (2014): *Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA*
http://www.wired.com/2014/04/obama-zero-day/
[17] Walsh, J (2014): *Free Can Make You Bleed*
http://www.ssh.com/blog/makesyoubleed
[18] Wikipedia: *National Security Agency*
https://en.wikipedia.org/wiki/National_Security_Agency
[19] Pras, A. et al (2010): *Attacks by 'Anonymous' WikiLeaks proponents not anonymous*
http://doc.utwente.nl/75331/1/2010-12-CTIT-TR.pdf
[20] van Rijswijk-Deij, R. et al (2014): *DNSSEC and its potential for DDoS attacks - a comprehensive measurement study,* Proceedings of the 14th ACM Internet Measurements Conference, IMC'14
[21] Cloudflare (2014): *Technical Details Behind a 400Gbps NTP Amplification DDoS Attack*
http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/
[22] Santanna, J.J. et al (2015): *Booters - An Analysis of DDoS-as-a-Service Attacks*, submitted to IFIP/IEEE Integrated Network Management 2015, IM'15 (under review)
[23] Rossow, C. (2014): *Amplification Hell: Revisiting Network Protocols for DDoS Abuse*, Network and Distributed Systems Security Symposium, NDSS'14
[24] M. Kührer, M. et al (2014): *Exit from Hell? Reducing the Impact of Amplification DDoS Attacks*, 23rd USENIX Security Symposium, USENIX'14
[25] Ferguson, P. (2000): *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, IETF BCP38

[26] Factsheet Investeringen in R&D (2012): *Investeren in onderzoek en innovatie is cruciaal voor de economische groei*, VSNU
http://www.vsnu.nl/files/documenten/Factsheets/01_Factsheet_-_Investeren.pdf
[27] Vervoort, W.A. (2006): *Informatica aan de THT*, Universiteit Twente, ISBN 90-365-2354-0
http://www.utwente.nl/ewi/geschiedenisinf/
[28] Wikipedia: Wetenschappelijk onderzoek
http://nl.wikipedia.org/wiki/Wetenschappelijk_onderzoek
[29] IFIP TC6 Open Digital Library
http://opendl.ifip-tc6.org