Ongebreidelde functionaliteit grootste vijand beveiliging

Automatisering Gids #39, 24/9/2004, p.15.

Bart Jacobs,
Hoogleraar Beveiliging en Correctheid van Programmatuur,
Nijmeegs Instituut voor Informatica en Informatiekunde (NIII),
Radboud Universiteit.

Open source kan bijdragen aan de beveiliging van computersystemen. Evenals de soberheid van die systemen. Het grootste gevaar, constateert de beveiligingsexpert Bart Jacobs, is te veel functionaliteit. ``Uit beveiligingsoogpunt zou een sobere Spartaanse aanpak het beste zijn.''

Computer security is tegenwoordig een hot topic. Security is gebaat bij sobere en Spartaanse computersystemen, en niet bij ongebreidelde functionaliteit. Openheid, bijv. via open source, kan ook aan beveiliging bijdragen, simpelweg omdat met de huidige stand van de techniek foutvrije software niet gegarandeerd kan worden. Evaluatie van computersystemen is een gebied waarop Nederland de mogelijkheden heeft om een rol van betekenis te spelen.

Het is duidelijk dat we met z'n allen steeds afhankelijker zijn geworden van computers, voor bewerking en beheer van documenten, voor communicatie en voor de besturing en regeling van velerlei processen. Daarbij zijn veel zaken ``gevoelig'' en ``waardevol'', in brede zin. Het vak computer security gaat over het reguleren van toegang tot zulke waardevolle zaken, zodat partijen bijvoorbeeld alleen die gegevens (of software) kunnen inzien (of veranderen) waartoe ze geautoriseerd zijn. Dit roept direct een aantal fundamentele vragen van het vakgebied op: hoe stel je vast wie je tegenover je hebt en wat de bevoegdheden zijn (zowel van mensen als van computerprocessen)? Hoe scherm je af voor ongeautoriseerde partijen? En ook: hoe en door wie worden authenticatiemiddelen en bevoegdheden eigenlijk toegekend, en weer ingetrokken?

Zwakheden

Het belangrijkste gereedschap voor computer security is cryptografie, de wiskundige discipline die technieken levert voor het versleutelen en ontsleutelen van gegevens. Een versleutelingsmechanisme (zoals AES of RSA) wordt typisch geparametriseerd door een cryptografische sleutel. Dit is een bepaald getal, waarvan de grootte (en daarmee de sterkte) gewoonlijk in bits wordt uitgedrukt. Alleen iemand in het bezit van de juiste sleutel kan een versleuteld document ontcijferen, of van een digitale handtekening voorzien. Zulke cryptografische sleutels dienen dus zelf weer beschermd te worden bijv. via een wachtwoord of vingerafdruk (op een gewone computer) of een pincode (op een chipkaart). Cryptografie is jarenlang vooral beoefend door militairen en diplomaten, maar is sinds de jaren zestig ook een belangrijk hulpmiddel voor de industrie (bijv. voor banken) en burgers (bijv. in GSM telefoons). Voor langere tijd viel het gebied computer security grotendeels samen met cryptografie.

Echter, wanneer we gaan kijken waar de laatste jaren dingen fout gaan, dan blijkt dat zelden aan de crypto te liggen. De zwakheden worden meestal veroorzaakt door falende software of door onjuist menselijk handelen. Security blijkt een breed, multidisciplinair gebied te zijn waarbij niet alleen de techniek een belangrijke rol speelt: juiste

procedures en inrichting van processen, opsporingsfaciliteiten en een afdoende juridisch kader zijn minstens zo belangrijk. Een voorbeeld van een elementaire beveiligingsprocedure binnen een bancaire context is: voor grote overboekingen zijn de handtekeningen van twee senior medewerkers nodig is. In het algemeen vraagt beveiliging om een juiste mix van technische, organisatorische en juridische maatregelen.

Verschuiving

Bij de technieken die gebruikt worden voor computerbeveiliging is er de laatste jaren een nadrukkelijke verschuiving zichtbaar van wiskunde richting informatica, door de afname van het relatieve belang van cryptografie. Informatici gebruiken cryptografische technieken meestal als black box, via voorgeprogrammeerde programmabibliotheken, zonder zich veel zorgen te maken over de wiskundige details. De daadwerkelijke implementatie van beveiligingsmechanismen in computers brengt heel eigen (informatica)vragen met zich mee, zoals: hoe zoek je in een database met versleutelde gegevens? Hoe reguleer je toegang in een file systeem? Hoe regel je het sleutelbeheer? Hoe produceer je een correcte implementatie van een bepaald security protocol? Hoe bescherm je een webserver tegen aanvallen? Computer security is ook binnen de informatica een zeer breed onderwerp, dat van belang is in velerlei subdisciplines, zoals besturingssystemen, netwerken, databases etc.

Opvallend aan het gebied computer security is de relatief grote nadruk die gelegd wordt op certificering. Het is niet genoeg om enkel een goed beveiligd systeem te bouwen: het moet ook aantoonbaar goed beveiligd zijn. Het systeem moet vertrouwd kunnen worden. Binnen met name de militaire en bancaire context zijn hiervoor speciale certificatiemechanismen ontwikkeld, waarvan de zogenaamde Common Criteria waarschijnlijk de bekendste zijn. Een Common Criteria evaluatie (of ``stempel'') is echter een niet-triviale aangelegenheid, waar extra tijd (en geld) voor uitgetrokken moet worden. In Nederland kunnen zulke evaluatie worden uitgevoerd door TNO ITSEF.

Waarom zijn er zoveel beveiligingsincidenten---met virussen, wormen, inbraken, defacements van webpagina's etc? In het algemeen gaat het hier om een combinatie van: gebrek aan aandacht voor beveiliging, en een gebrek aan effectiviteit van bestaande beveiligingsmechanismen. In het vervolg zullen deze twee aspecten nader belicht worden, vooral vanuit technisch perspectief.

Grootste vijand

Het bestaande gebrek aan aandacht voor beveiliging heeft vele oorzaken. Natuurlijk, beveiliging is lastig voor de gemiddelde gebruiker, en vertraagt de beoogde voortgang, en dient daardoor zoveel mogelijk vanzelf te werken. Maar de grootste vijand van beveiliging is ongebreidelde functionaliteit. Fabrikanten menen meer producten te kunnen te verkopen door steeds meer functies toe te voegen. Er is niemand die zegt: ``kijk dit fantastische product van mij: het is hardstikke veilig, maar het kan bijna niks!''. Zo'n sobere Spartaanse aanpak zou wel het beste zijn---vanuit beveiligingsperspectief.

Het grootste voorbeeld van uit de hand gelopen functionaliteit is de welbekende PC. Bekijk alleen eens wat een testverwerker als MSWord voor functies biedt, zeker wanneer daarbij macros meegenomen worden. Hoeveel van deze functionaliteit wordt regelmatig gebruikt? Al deze mogelijkheden (en combinaties daarvan) bieden echter aanknopingspunten voor misbruik. Met de mobiele telefoon gaat het dezelfde kant op: het platvorm van een gemiddelde GSM is inmiddels zo complex, met software van zoveel verschillende partijen, dat het

overzicht op de mogelijke vormen van exploitatie snel verloren gaat.

Het is dus verstandig om dergelijke complexe multi-purpose systemen niet voor critische beveiligingstaken te gebruiken. Men kan zich dan ook afvragen of een digitale handtekening die via een gewone PC door een chipkaart gezet is wel betrouwbaar is. Er zou immers een virus op de PC actief kunnen zijn dat de de PIN code van de chipkaart achterhaald heeft via het registreren van toetsaanslagen, en daarmee volledige controle over de chipkaart heeft. Of een virus dat een ander document op het scherm toont dan ter ondertekening naar de chipkaart gestuurd wordt. Het is een kwestie van wachten op de eerste jurisprudentie over dergelijke zaken: wat zal de rechter zeggen wanneer ik claim dat niet ik digitaal getekend heb maar een kwaardaardig virus? In plaats van een multi-purpose PC zou men liever een single-purpose (gecertificeerd) apparaat willen gebruiken dat simpel en overzichtelijk werkt: een A4-display met een kaartlezer en keypad in tamper-proof (of resistant) hardware, met e'e'n enkel (bijv. infrarood) communicatiekanaal voor het up- en down-loaden van documenten, in slechts e'e'n standaard formaat. Sober en Spartaans, natuurlijk zonder mogelijkheid van software updates! Is daar een markt voor? Een betere vraag is: is het beveiligingsbewustzijn inmiddels zodanig dat dergelijke apparaten als noodzakelijk gezien worden?

Soberheid

De volgende vraag is dan natuurlijk naar de effectiviteit van bestaande beveiligingsmechanismen: is de stand van de techniek zodanig dat dergelijke apparaten met voldoende mate van betrouwbaarheid geproduceerd kunnen worden? Een simpel antwoord op deze vraag is niet te geven. In plaats daarvan noemen we de volgende, vooral negatieve, aspecten.

- Security is niet een eigenschap die aan het eind van een ontwikkeltraject nog even toegevoegd kan worden, maar moet van meet van aan in het ontwerp opgenomen worden.

- Security eigenschappen zijn moeilijk testbaar: hoe vind je bijvoorbeeld een geheime toetsencombinatie die een backdoor activeert?

- Security en complexiteit gaan niet samen.

- Foutloos programmeren (of specificeren) bestaat niet.

- De huidige formele validatiemethoden zijn onvoldoende krachtig (en schaalbaar) om correctheid van niet-triviale realistische systemen te garanderen---behalve na agressieve abstractie.

Het geschetste beeld is somber. De (certificatie) praktijk komt inderdaad vaak niet verder dan het nalopen van een aantal standaardlijsten (zoals bijv. de Code voor Informatiebeveiliging van het Genootschap van Informatie Beveiligers GVIB), zonder tot volledige dekking te komen. Het is dan ook de grote uitdaging aan de gemeenschap van onderzoekers op computer security gebied om het gat te verkleinen tussen enerzijds het controleren met behulp van deze concrete checklijsten en anderzijds het gebruiken van formele methoden op abstracte modellen.

Een pragmatische uitweg lijkt geboden te worden door een radicale acceptatie van de beperkingen van certificatiemethoden en de werking van het gehele systeem openbaar te maken, typisch via de ``open source'' aanpak. In eerste instantie lijken openheid en beveiliging slecht samen te gaan. De impliciete vooronderstelling daarbij is dat datgene wat men ``onder de pet'' wil houden ook correct is. Wanneer

men daarvan niet verzekerd is, is openheid een goed alternatief, waarbij veel (goedwillende) controleurs (``many eyeballs'') kunnen zorgen voor snelle identificatie en reparatie van mogelijke fouten.

Reputatie

Tenslotte, wat kunnen en moeten wij in Nederland op het gebied van computer security doen? Onze middelen zijn beperkt, en onze expertise is, net als elders, verspreid over gemeenschappen die onderling beperkt communiceren: inlichtingendiensten, specifieke bedrijven (waaronder banken, electronicaproducenten, automatiseerders, gespecialiseerde leveranciers) en (academische) onderzoeksinstellingen. Sinds een paar jaar zijn er een aantal innovatieve landelijke projecten voor betere samenwerking (SAFE-NL) en stimulering (Sentinels van STW) op onderzoeksgebied. Het lijkt sowieso verstandig een minimale ontwikkelcapaciteit voorhanden te hebben, om niet voor strategische taken van het buitenland afhankelijk te zijn---met alle risico's van backdoors. Daarnaast zijn er voor de hand liggende mogelijkheden voor Nederland op certificatiegebied. We hebben wereldwijd een redelijk onafhankelijke reputatie, bijvoorbeeld als gastland van het internationale gerechtshof in Den Haag. Het maakt in de beeldvorming veel uit of een Franse chipkaart door een Franse of door een Nederlandse evaluator beoordeeld is. We hebben in Nederland een sterke traditie in formele methoden aan de universiteiten en het is een grote uitdaging om die expertise uit te bouwen en in te zetten ten behoeve van het ontwikkelen en toekennen van internationaal erkende keurmerken. Met gerichte sturing en steun ligt hier een voor de hand liggende rol voor kennisinstellingen als TNO en universiteiten---bijvoorbeeld met de evaluatieactiviteiten van de Nijmeegse Security of Systems (SoS) groep en van het Eindhovense Laboratory for Quality Software (LaQuSo). Daar kan een klein land groot in zijn!

Kaders

Wetgeving

Op het gebied van wetgeving is er het laatste decennium veel veranderd in Nederland, door de opname van verschillende bepalingen over computercriminaliteit in het wetboek van strafrecht---zoals art. 138a Sr: over computervredebreuk (hacken), of art. 350a Sr: over het wijzigen of vernietigen van opgeslagen gegevens. Echter, door beperkte ervaring en kennis van zaken bij de politie het en openbaar ministerie, worden deze wetten nauwelijks toegepast. Civielrechtelijk kan ook e'e'n en ander geregeld worden, zoals bijvoorbeeld in de gebruiksvoorwaarden voor bankpassen, waardoor eventueel misbruik van klanten leidt tot aansprakelijkheid.

Staatsgeheimen

Hoe kan openheid bijdragen aan beveiliging? Twee voorbeelden illustreren deze vraag. Stel je gaat naar slotenmaker 1, die zegt: ``hier heb ik een fantastisch deurslot. Hoe het werkt kan ik niet vertellen, want dan zouden inbrekers van die informatie misbruik kunnen maken. Maar vertrouw me maar, het is echt veilig!''. Slotenmaker 2 zegt: ``ik heb ook een goed slot: iedereen kan dat zelf zien, het werkt namelijk zo en zo. De beveiliging hangt niet van dit mechanisme af, maar puur van de complexiteit (aantal groefjes en zo) van de sleutel.'' Wie vertrouwt U meer: de eerste of tweede sleutelmaker?

Een groot beveiligingsrisico wordt altijd gevormd door backdoors: achterdeurtjes in programmatuur die heimelijk toegang kunnen verlenen aan de ontwikkelaars. Men kan zich afvragen of bijvoorbeeld Nederlandse staatsgeheimen (zover in digitale vorm) door software afgehandeld moeten worden waarvan de preciese werking aan geen enkele Nederlander bekend is (zoals bij Windows besturingssystemen). In de plaats van staatsgeheimen kan men natuurlijk ook denken aan cruciale industriele geheimen, of ook aan aftapgegevens van politie.

`Heb je even tijd?'

Organisatorische beveiligingsmaatregelen behelsen bijvoorbeeld het dragen van badges of het op een bepaalde manier omgaan met wachtwoorden of attachments. Ze zijn zeer belangrijk, maar vragen veel discipline. In de praktijk worden procedures vaak omzeilt uit gemakzucht, onwetendheid, of uit nonchalance. Social engineers kunnen hier dankbaar gebruik van maken: mensen zijn over het algemeen vriendelijk en meegaand, zeker wanneer iemand in de problemen lijkt te zitten. Social engineers doen zich vaak voor als insiders, en weten via onschuldig lijkende vragen cruciale informatie te ontfutselen. Bijvoorbeeld over de telefoon: ``Hallo, ik ben van systeembeheer, en hoor dat je hier nieuw bent. Heb je even tijd om de beveiligingsprocedures door te lopen? [...] Je moet natuurlijk een sterk wachtwoord kiezen, want [...] Wat gebruik je nu? Als je er dat van maakt is het stuk sterker. Weet je hoe dat moet? [...]''. Wat in feite nodig is, is constante paranoia: is dit bericht (of telefoontje) wel echt afkomstig van de vermeende afzender? Wie heeft de inhoud onderweg gezien, of kunnen veranderen, enz. Echter, zonder spionnenopleiding houdt bijna niemand dat vol. Goede training en beloning, en regelmatige herinneringen en opfriscursussen kunnen wel degelijk verschil uitmaken.