



TEKNILLINEN KORKEAKOULU

Active Content, E-commerce and Convergence Security



- Executable content
- E-commerce and web security
- Convergence of telecommunications and data communications



Executable Content

- Data is received from some outside source and executed as a program on the client host
 - Automatic execution
 - Usually received from a WWW page
- Executable content is a potentially powerful technology and keeps on appearing in different forms
 - Agents
 - Active networks
 - Proxlets



Problems With Executable Content

- Computation is moved to the client
- The problem area is related to malware
- Clients need to be protected from rogue service providers
- End users are forced to become administrators and policy makers
- Mobile (agent) code moves from host to host, executing a task given to it
 - Clients must be protected from malicious mobile applications
 - The mobile code must be protected from a malicious host



Signed Code

- The program is digitally signed
- Signature keys are certified
- The browsers come with certification root keys
 - It is easy to delete and add more root keys
- With signed code, you probably know who wrote the program
- However, you do not know if the code is malicious or not



- Microsoft active technology
- Basically very little security
- Idea of small controls, i.e. functional components
 - Buttons, labels, charts etc
- Loaded from disk, if not there fetched from the net
 - An ActiveX component is signed by a vendor and the signature is checked by the client software using an included certificate and PKI structure
- What about signed but malicious controls?
 - Examples can be found



ActiveX Authenticode

- Microsoft's solution for securing executable content
- Code is signed
- Browser asks user whether to allow the downloaded code to run or not
- If the user accepts the certificate, the software is allowed to run without any restrictions
 - It could delete all your files
- Problem: users often want to try a program even if they do not trust its source



- Sun Java technology
- Java is many things
 - An object oriented programming language
 - Run time environment
- Client executable code is called an applet
- Applets may come from any source
- Users may want to securely run code they do not trust (they might not even know where it came from)
- The Java programming language was designed with security in mind
 - Byte code verifier, class loader & security manager
- Implementations in browsers have had serious bugs



Security Model of a Java Applet

- Java is a general purpose language, here we are looking at applet use
- Classloader in the run time environment differentiates between local (trusted) and network (applet) code
 - Local class is (should be) always preferred to network class
- Verifier checks the byte code
 - Byte code is the binary code compiled from the Java source code and native to the Java Virtual Machine
 - The Verifier attempts to find stack over and under flows, checks correct use of variable types and generally the syntax of the byte code
- SecurityManager implements the Java sandbox
 - Sandbox limits the applet's actions severely



The Java Sandbox

- The applet in the sandbox may not:
 - Read or write files
 - Open network connections to hosts other than the originating host
 - Initiate execution of new processes or programs
 - Use any native methods
- Only trusted code (local classes) can use the OS services
 - Local library classes check if they are called from the sandbox or from a local applet running outside the sandbox
- Signed applets can exceed the sandbox limitations



- Not related to Java
- A scripting language created by Netscape used in Web pages
- Microsoft has a non-compatible Jscript
- WAP has WMLscript
- More limited action possibilities than Java/ActiveX
- However, no sandbox-like security features!



Server Side Code

- Code is executed in the server
 - Bugs can compromise the server (intrusions)
 - Execution requires computational resources from the server (denial of service)
- Many scripts are written by people who know little or nothing about security
- If you are using CGI scripts or servlets (server side applets):
 - Keep track of what scripts you have, remove the ones you do not need
 - Control the access rights the scripts have (don't run them as root or administrator)
 - Do source code security review if possible



Securing E-commerce

- E-commerce is an application over some infrastructure, like the Internet
- As an application it has several security needs
 - Security of the serving infrastructure technology
 - Security of the information in the server
 - Security of the transaction
 - Non-repudiation needs



Types of E-Commerce

- **Business to Business**
 - Typically medium size to large transactions and long term relationships
- **Business to Consumer**
 - Typically small to medium size transactions and loose relationships
- **Consumer to Consumer**
 - Typically small to medium size transactions, lack of trust between the parties and no prior relationships
- **Different types of commerce prefer different solutions**



E-Commerce Servers

- WWW and e-mail are the most common applications
- Standard firewall and host security solutions can be used to secure the server
- The server often contains credit card information, customer addresses, business confidential data, pending orders etc.
 - Some credit card companies already require that the credit card information is located in a separate server
 - Front and back-end server architecture
 - Threatens both to confidentiality and integrity



E-commerce Transactions

- Identifying the participants is often required
 - SSL authenticates the server
 - PKI systems could be used to authenticate both participants (once they are in global use)
 - PGP and S/MIME could be used, but are rarely used
 - Extranets can use PKI or usernames and passwords
 - Sometimes it is easiest to accept a certain amount of losses
- There are formal standards for B2B commerce
 - EDI/OVT
 - XML-based standards are emerging
 - PKI-based signatures are beginning to be used



Non-repudiation in E-commerce

- PKI systems could provide electronic signatures
 - Many countries have laws about these
- What happens if the signer repudiates the signature?
 - The whole system may be evaluated in public court
- Transaction logs can be useful
- Instead of non-repudiation, how about pre-payment
 - In Finland the banks have rather flexible online systems
 - The credit card companies have different solutions, too
 - Remember that WWW forms and cookies are freely editable by the user



Convergence of Telecommunications and Internet

- Internet and traditional telecommunications networks and services are converging
 - Called NGN, Next Generation Network
- As systems they are very different
 - Telecoms network is one big machine, where all intelligence is in the network
 - Internet is a simple message passing network, where all intelligence is on the edges
- This will cause security problems



Security in Telecom Networks

- Separate user and control planes
 - Misuse very difficult
 - Occasionally possible, e.g. hacking of in-band signaling
- Signaling security
 - Most of the signaling is in a separate network (control plane, implemented using SS7)
- Signaling is truly international
 - Between operators and countries
- Most critical services and components are duplicated
- Bits in telecoms mean money, therefore good security built in



- Parts or all of the telephone bearer network are being replaced with IP networks
- Internet VoIP calls are routed to the telephone system
 - SIP (Session Initiation Protocol) to initiate the call
- UMTS will have an IPv6 internal network
 - Possibly with virtual operator's equipment
- UMTS will also have the IMS (IP Multimedia Subsystem) to replace MSC (Mobile Switching Center)



Integration and New Problems

- No more user/control plane separation
 - Signaling and user data intermixed
 - Caller's telephone number can no longer be trusted
 - As it is delivered with SIP over the Internet
- Borders and responsibilities between operators blurred
- Terminal equipment much more intelligent
- Networks extended to customer premises
 - Physical protection not any more the same



Future View: Basic Security After Convergence

- Data and Telecom Networks integrated
 - Signaling integrated, accounting combined
 - Signaling protected cryptographically
- Accounting integrated
 - Visionaries say through a millcent system like ecash in order to reduce delay
 - Or flat fee for basic services
- Firewalls everywhere
- User data protected cryptographically
- Management will be a large problem
 - How to manage cryptographic keys?
 - How to manage firewall access control?



Future of Security

- Cryptography and PKI are seen currently as the silver bullet to solve all problems
 - PKI is more complex than originally thought
- It has been said that this is the “golden age” of hacking and cracking
 - Current and future systems will have security included from the start of the design process, not as an afterthought
- In the future security services are going to be more clearly defined and easily available
 - Security is an infrastructure service
- However implementing security will continue to require know-how in the foreseeable future