Electronic Industrial Espionage:
A Report From Ground Zero

Ira S. Winkler
National Computer Security Association
10 South Courthouse Avenue
Carlisle, Pennsylvania 17013
(717) 258-1816
(717) 243-8642 (fax)
winkler@ncsa.com

Agenda

- What is Electronic Industrial Espionage?
- Who would do it?
- Methods
- Case Study of an Industrial Espionage
- How can it be prevented?

What is Industrial Espionage?

- Compromising trade secrets through any means possible for economic, or possibly military, gain
  - Legal and illicit
- Referred to as Economic Espionage when performed by a foreign government
- *They will take information in any form*
- *They will attack you where you are weakest*

Electronic Industrial Espionage

- The use of technical means to obtain trade secrets
- May be combined with non-technical methods to enhance results of either
- Significantly reduced risk
  - Less exposure and direct contact
  - Less likely to be caught and pursued

Who Would Do It?

- **Primarily Outsiders**
  - –Competitors
  - –Legal rivals
  - –Freelancers
  - –Organized Crime
  - –Hackers
  - –Private Detectives
  - –Information Brokers

Who Else?

- Foreign Intelligence Services
  - Economic Espionage
  - Every company has potential military relations
- They will use more sophisticated methods
  - Combine with insider activities
  - Much better funded and organized

Methods

- Insiders do "Insider Things"
- Insiders are generally motivated by greed and will not ask for outsider help . Also they risk exposure if they ask for help
- Outsiders do not want to risk exposure by soliciting insider support
- Takes a little longer

Surprise

- Almost all methods are easily prevented or detected
- The work is not that of a James Bond or Super Genius; it is that of Kevin Mitnick
- A monkey can do it

Methods

- Technical hacking
  - Compromise of very known vulnerabilities
  - Use attacks straight off the Internet
  - Two bit criminals to intelligence agencies use these almost primarily
  - Few "groups" have the capability to develop their own capabilities
- Telephone taps
  - Either pay people off (MoD, Mitnick) or hack the phone companies yourself
  - Foreign intelligence capability is widely known

Methods

- Network sniffing
  - Tools widely available
- TEMPEST radiation
  - Conversion of a television set
  - Kits available from $800
- PBX Hacking
  - Same as technical hacking
  - Gives access to voice mail

Methods

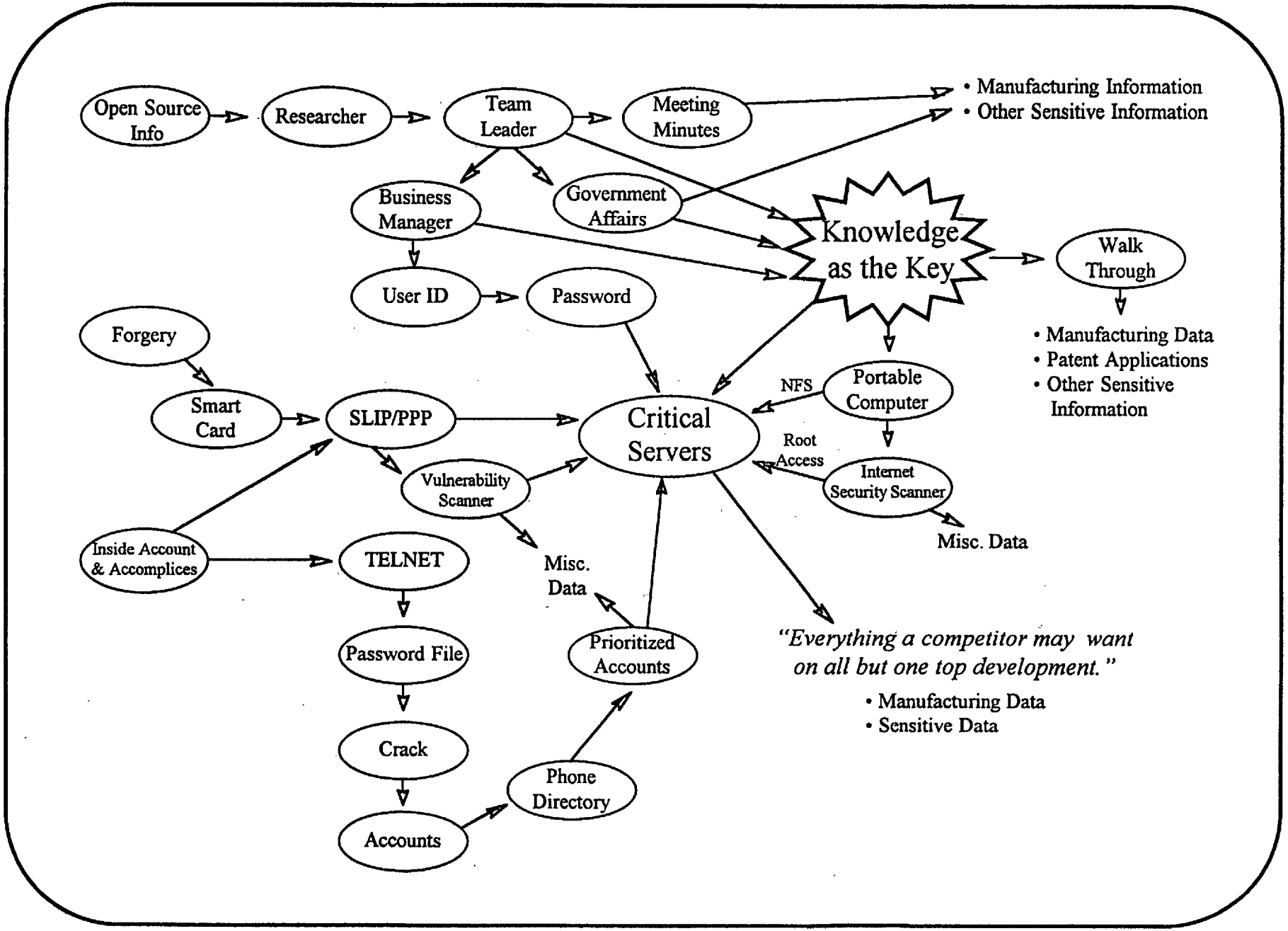
- **Bugging**
  - **Bugs are inexpensive**
  - **15 - 33% of companies, that are tested, find bugs**

Case Study

- Placement of a person as a temporary employee in a high tech firm
- Full scale industrial espionage simulation
- No holds barred attack
- Multi-faceted attack
  - Open source research
  - Misrepresentation
  - Walk through facilities
  - Internal hacking
  - Internal coordination of external accomplices

Background

- Company has many emerging developments
- Developments valued in excess of $10 Billion by Wall Street analysts
- Company has experienced several cases of industrial espionage
- Research mentality of openness causes an operational security nightmare
- Security manager is very well aware of the threat
  - Secures what he can


Open Source Info
Researcher
Team Leader
Meeting Minutes
• Manufacturing Information
• Other Sensitive Information
Business Manager
Government Affairs
Knowledge as the Key
Walk Through
• Manufacturing Data
• Patent Applications
• Other Sensitive Information
User ID
Password
Forgery
Smart Card
SLIP/PPP
Critical Servers
NFS
Portable Computer
Root Access
Internet Security Scanner
Misc. Data
Vulnerability Scanner
Misc. Data
Inside Account & Accomplices
TELNET
Password File
Prioritized Accounts
"Everything a competitor may want on all but one top development."
• Manufacturing Data
• Sensitive Data
Crack
Phone Directory
Accounts

Results

- All but one emerging development was seriously compromised
- Information valued in the billions of dollars
- Pending litigation posture compromised
- Patent applications compromised
- What else is there to say

15

Believe it or Not

- *Critical compromises accomplished within one and a half days*
- *No reports of any activities*
- They have much better than average security
  - Technical Security
  - Physical Security

Preventing Espionage

- Good, basic System Administration
  - Doing simple things that should be done anyway
  - Update systems as vulnerabilities are announced
  - CERT, CIAC, IS/Recon type services
- Use available mechanisms
  - Most systems have security features that are not turned on
- Use Operations Security procedures
  - Use Intelligence principles to not talk about things over the telephone

Preventing Espionage

- Perform Bug Sweeps
  - Yeah, maybe they won't turn up anything, but...
- Every so often examine network resources

18

Conclusion

- You will be a victim
- An idiot can do a good job getting into your company
- Good procedures can stop it

19

Information Security is *Information* Security

20

OSS '96: THE CONFERENCE Proceedings, 1996 Volume II, Fifth Internatinal Symposium Global Security & Global Competitiveess: Open - Link Page

Previous	Appreciation and Table of Contents
Next	Mr. William Ruh, Senior Vice President, Center for Information Technology, Concept Five Technologies, Optimizing Corporate Capital Through Information Technology

Return to Electronic Index Page