RSACONFERENCE2010

SECURITY DECODED

State of the Art Automation of Open Source Intelligence and Impersonation in Social Networks

Pedro O. Varangot
Core Security Technologies

Session ID: RR-303
Session Classification: Advanced

Agenda

- Introduction to OSINT and SNN
- The Attackers Perspective
- Exomind
- An Example Attack

Introduction

Open Source Intelligence

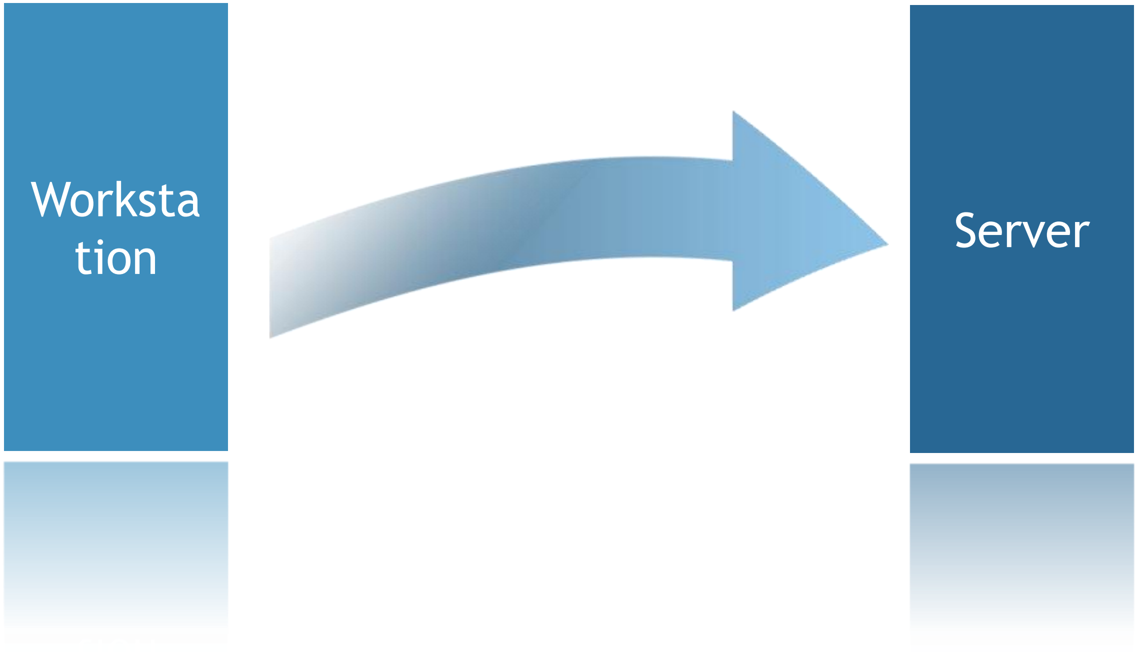
Social Networks

Basic concepts

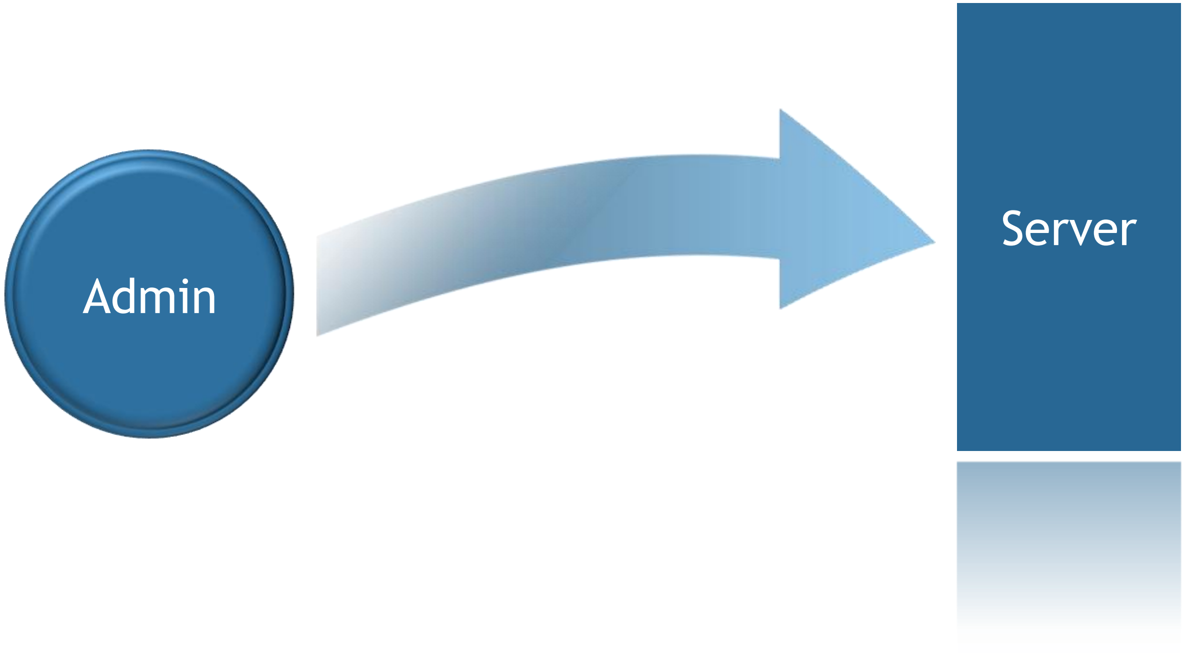
- **OSINT**: Passive Information Gathering

- **The Perimeter is Inside Out**: Client Side Attacks
  - XSS vulnerabilities
  - Browser/Plugin Exploits
  - Word, Excel, Powerpoint…
- **Relations of Trust**: abstraction of a very old concept in security

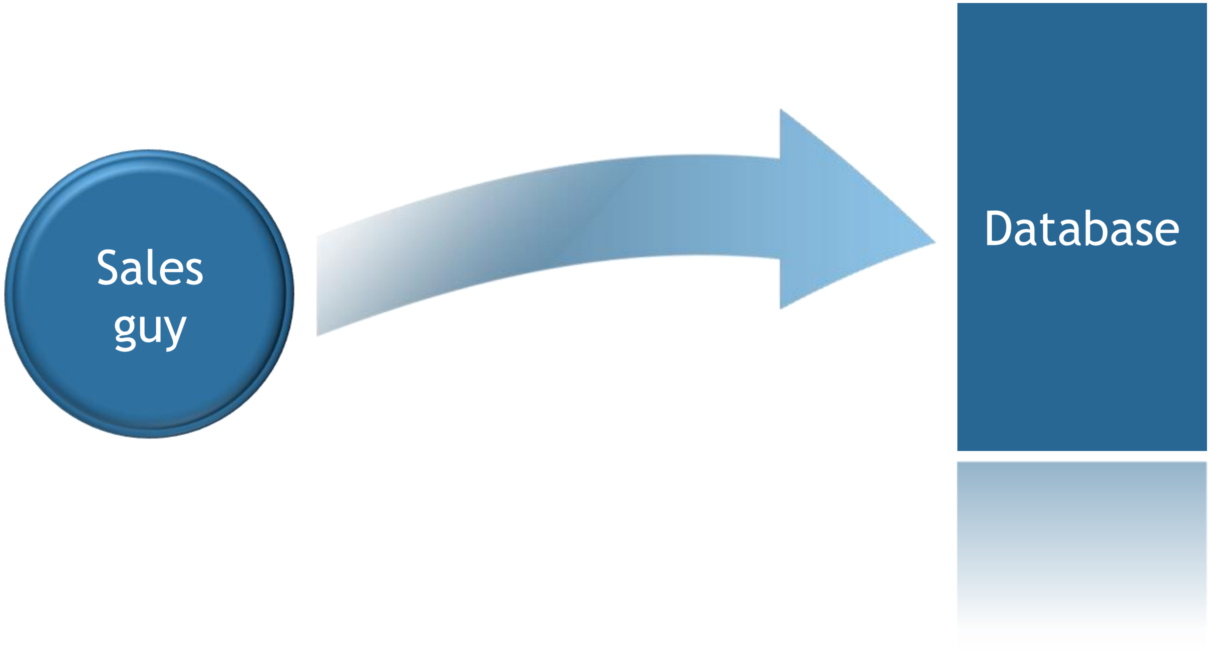
Trust relations



Trust relations



Trust relations



Social networks

- **Relations of Trust**: exposed on social networks
- Big database of who-trusts-who graphs
- Employee-Employer relation

Integration into “classic” pentesting

- At the “passive” information gathering phase of classical pentesting
- “Client Side Only” pentests getting popular
  - Most don t use OSINT gathered information
  - Even spear phishing still rare, though hot on the news

Going Mainstream

- Maltego (OSINT)
- Core Impact
- Metasploit

- Many other tools
  - theHarvester.py
  - PassiveRecon
  - Namechk
  - Binging

- (see Chris Gates @ BRUCON)

Social Networks

From the attackers perspective

Social networks

- More than passive information gathering

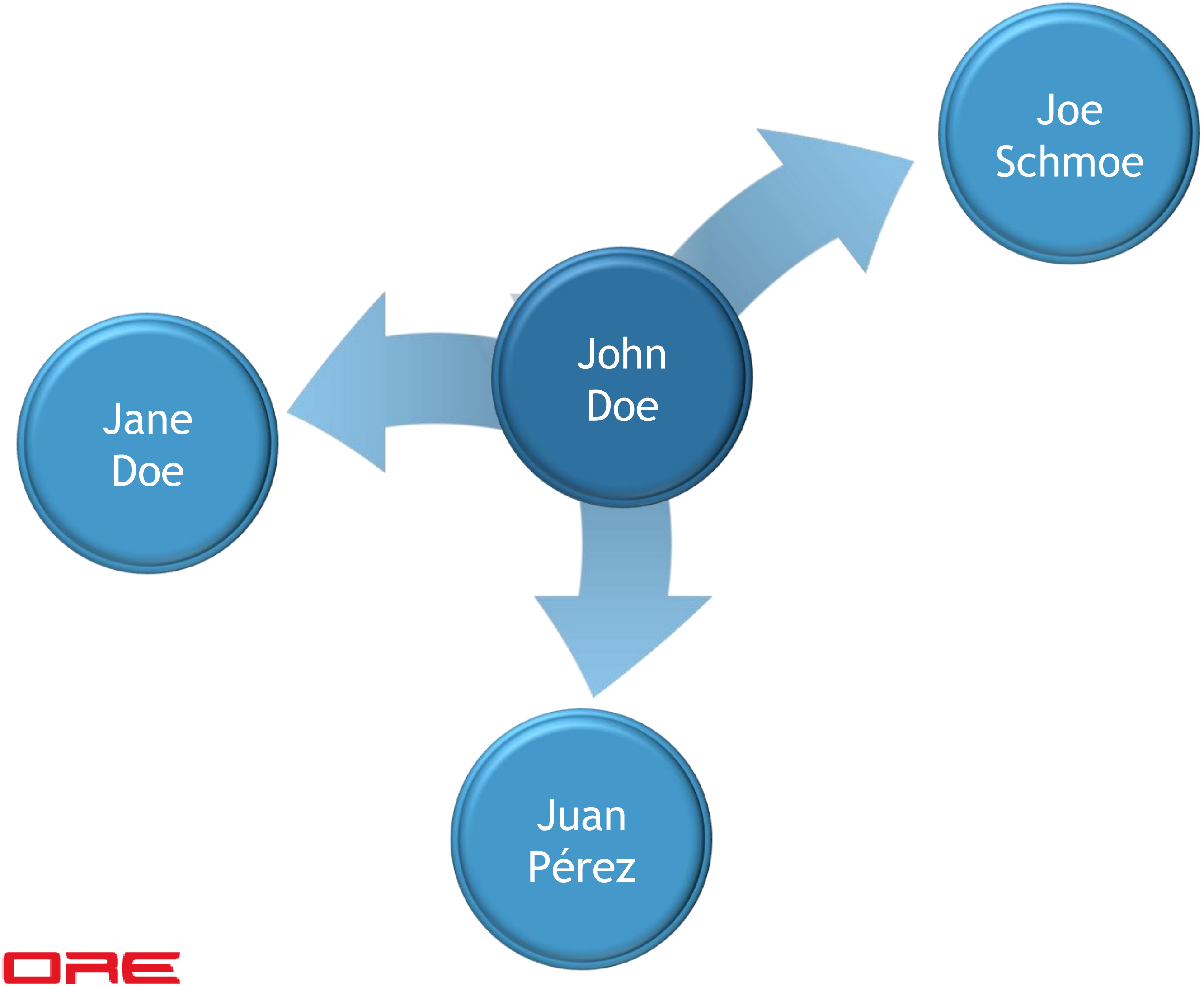
- Deployment platform for client-side exploits
  - **More accurate than bulk e-mail** for payload distribution
  - Or in any case, a gateway for perfected e-mail attacks (see Social Phishing or West Point carronade)
  - Easier to do impersonation attacks (if the attacker can handle the complexity)
  - Short url paradise (alltough a safer horizon can be seen)

Social networks

- Big database of trust relations

- Your identity online:
  - Profile data: name, picture, employer
  - Relations: **Contacts tell about who you are**

Contacts speak about who you are



Information on “need to socialize” basis

- Security: information given on a need-to-know basis

- Social Networks: “need to socialize” basis.
  - Giving information makes the network more useful to the end users.
  - But also to the attackers!

Back to pentesting

- Leverage information into spear-phishing attacks

- Go beyond spear-phising and e-mail
  - Use the social network as delivery channel.
  - **E-mail is now more suspicious to the user.**

- Core Security SCS has been using targeted attacks since 2002. Successfully.
  - Modern Intrusion Practices, Gera Richarte. Black Hat Vegas Briefings 2003.
  - Client Side Penetration Testing, Max Caceres. Black Hat Federal 2006.

Exomind

An extensible attack framework

What is Exomind?

- Prototype developed by José Orlicki (ITBA, CONICET) and me (Core Security). Part of a collaboration between CoreLabs and ITBA.
- Helps your brain (and fingers)
- **Direct gateway for attack payload delivery**
- Currently focused at network impersonation attacks
  - Chat bots.
  - Stochastic writing style analyzer.
  - Sub-network replication

Architecture

- Robust data model.
  - Fundamental to model the social graph and to expand support to more social networks.
- Extensible by “plugins”.
  - Expanders
  - Attacks
  - New social networks
- Lets see some code…

Example

- Complete twitter sub-network replication
  - Create a **complete fake profile (including followers)** to use as delivery medium for client side attacks. As realistically as we can.
  - Screenshots
  - Live demo on request (attacks take long to complete, and need many rounds of twitter API limits)

- We won t automatically create accounts. Neither will we help with it.
  - The same goes for e-mails.

- Aimed at automating a modern targeted advanced impersonation attack

The Future

- Testing on humans!
  - Expensive
  - Difficult
  - Unethical?

- Extend to support other social networks

- Integrate Core Impact/Metasploit to automate XSS or client-side vulnerability assessment

Thanks!

peter AT coresecurity.com

See also

- Keynote: The Evolution of Penetration Testing, Gera Richarte. SANS Pentesting Summit 2008.

- Open Source Information Gathering, Chris Gates. BRUCON 2008.
- LeakedOut: the Social Networks You Get Caught In, José Orlicki. BACON 2008.

- Social Phishing, 2005. Nataniel Johnson, Markus Jakobsson, Filippo Menczer.
- The West Point carronade, 2005. Aaron J. Ferguson.