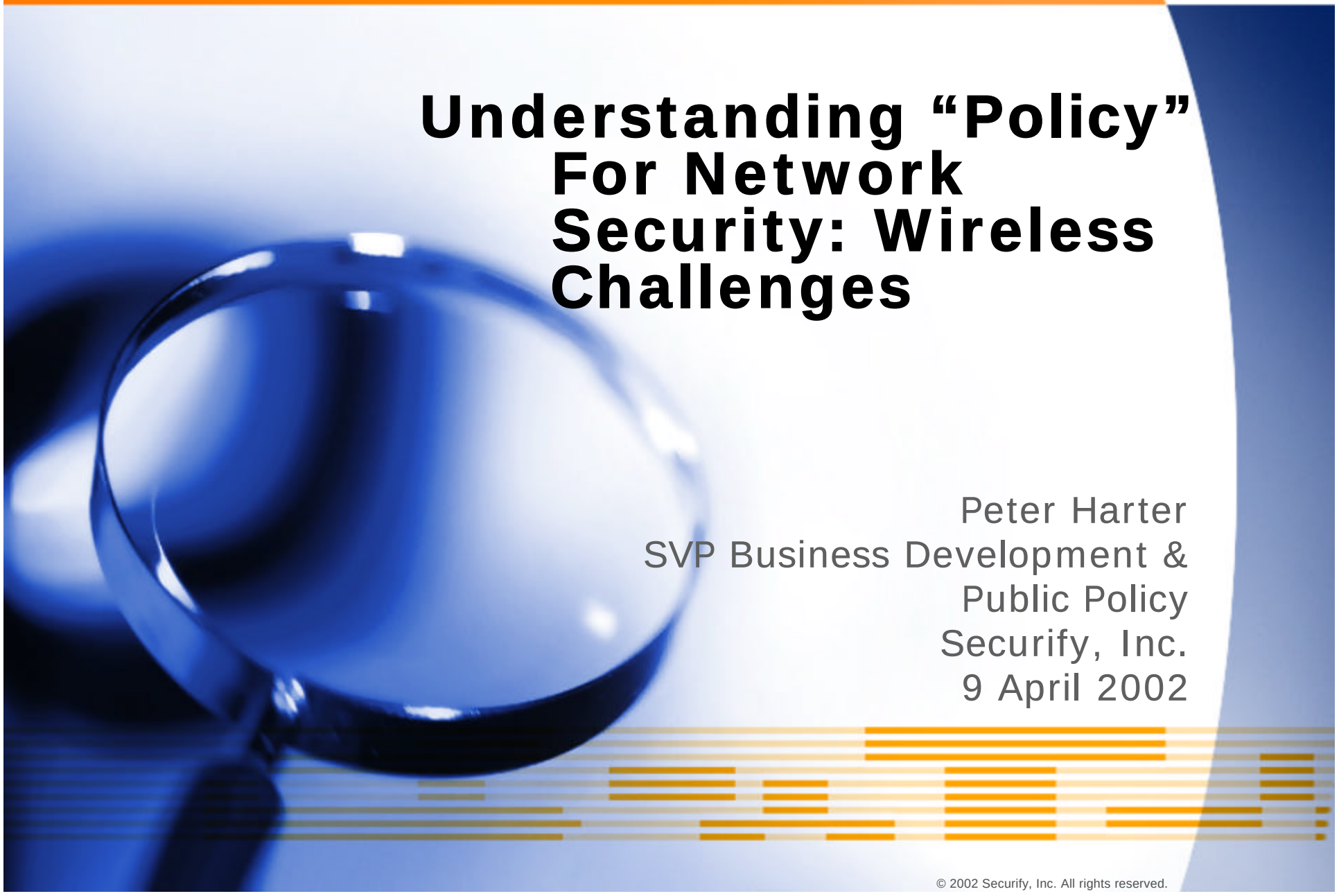
SECURIFY℠

Understanding "Policy" For Network Security: Wireless Challenges



Peter Harter
SVP Business Development &
Public Policy
Securify, Inc.
9 April 2002

Agenda

SECURIFY℠

- **Current environment**
- **Common problems**
- **Application and network security**
- **The need for change**
- **The wireless phenomenon and security effects**

Current Environment

SECURIFY

- **Where is the perimeter??**
- **ICC survey of wireless networks in London:**
  - 90% are exposed
  - Misconfiguration, default setting, weak or lack of encryption
  - Vulnerable to drive by access
- **Rogue networks and access points set up by employees**
- **PDAs and other handhelds have less power and facility and thus cannot handle PC based security solutions**
  - Eavesdropping and authenticating
  - Short range impersonation

The State of the IT Security Industry

SECURIFY

- **Success of the internet?**
  - We've been building the Internet for 25 years
  - Business & Government constantly use the Internet to improve efficiency:
    - To succeed in business today requires connectivity to customers, partners, and employees.
    - Hundreds of companies will put you on the net
    - Thousands of consultants will secure your net
  - Spending on security doubles every year
  - Losses and breaches increase every year
  - Loss due to security issues last year: $1.38 trillion (more than the GNP of France)*
- *We've got a problem*

*IDC, PwC

The State of the IT Security Industry

SECURIFY

- **Why do we have a problem?**
  - Business connectivity requirements have pushed technology beyond its limits:
    - Too many users
    - Too many machines
    - Too many security ‘solutions’
    - New uses come fast
    - Exploits come faster than patches
    - Great lack of expertise
- **To cope with this complexity**
  - technology is deployed to protect the network perimeter defending against known exploits, not the assets

Application or Network Security

SECURIFY℠

- Securing the application does not secure the data
- Can we use the same infrastructure to secure both the applications and the network
- Can the infrastructure extend to different types of clients
- A single framework for security is likely to produce the best results

The Need For Change

SECURIFY℠

- **Current Security Environment**
  - Concentrated at the Perimeter
  - Lots of Bad Guys, poor enforcement
  - Separate application and network security infrastructure
  - Hard to scale & manage
  - Checking for known signatures and viruses
    - Infinite number of unknown signatures & viruses
  - Vulnerability-based, not capability-based
  - Detects an attack, not a compromise
  - Security Product vendor is in control
  - Too much data and disconnected logs to analyze
  - Separate solutions for different problems that may have the same cause

A New Direction

SECURIFY

- **Operate networks like businesses – empower the network to understand the traffic and defend itself**
  - Capture the *business rules* that define how the network needs to work.
    - "Network security policy"
  - Compare the *actual operation* of the network with the *policy*.
  - Make correct business decisions based on actual vs. expected behavior.

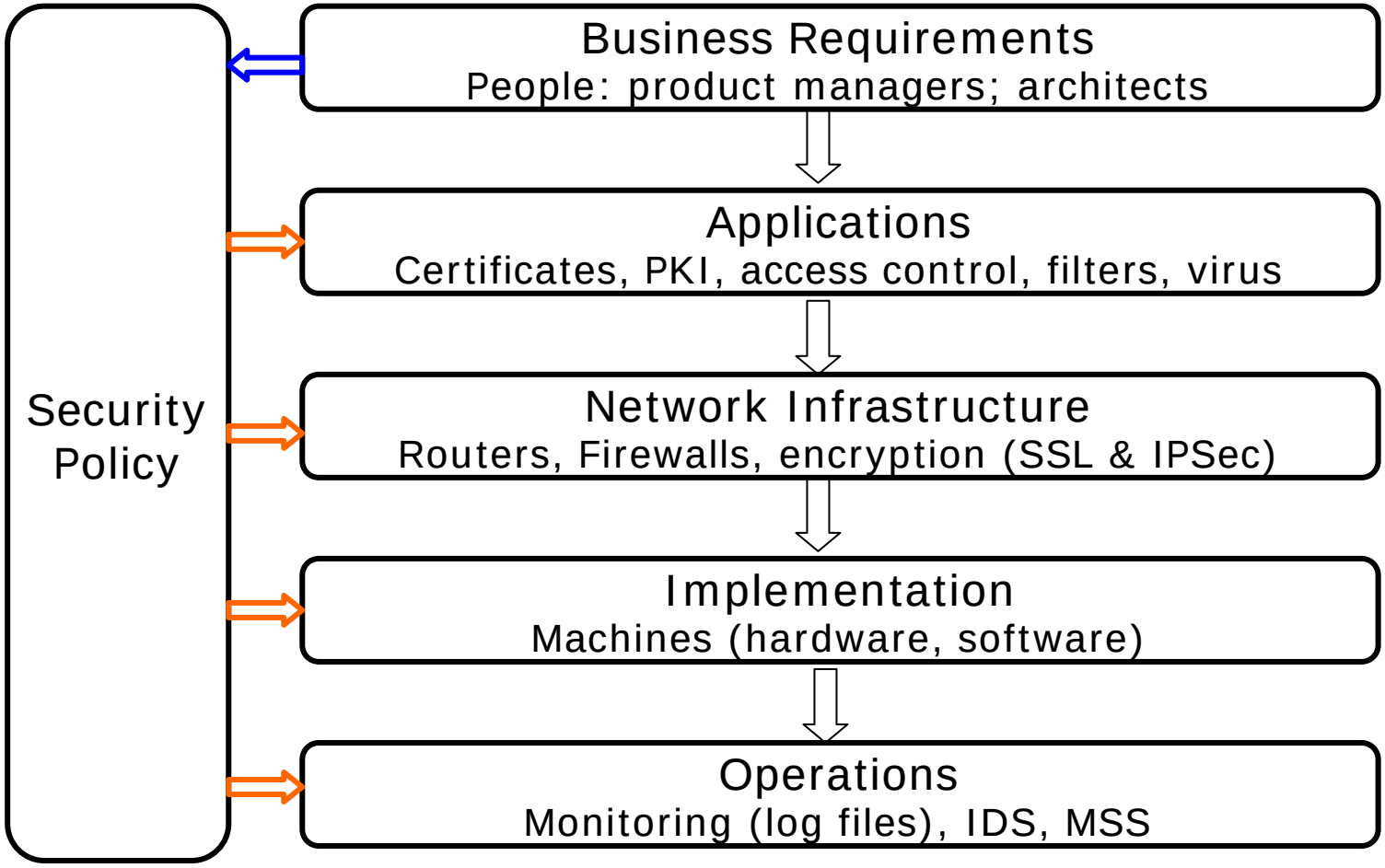
Traditional Network Security Services

SECURIFY

- **Analyze logs and other data from network devices**
  - How to identify rogue behavior
- **Investigate as many host machines and network devices as possible**
- **Conduct vulnerability assessments regularly**
- **All these are important – but where do the business-specific issues get handled**

The Policy-Empowered Network

SECURIFY



The Technical Breakthrough

SECURIFY℠

- Automation of the policy development process (from a business point of view, at all protocol layers)
- Derive policy automatically from configuration information that I know already
  - e.g., ‘What is this server supposed to do?’
- The policy is a *live document* on my computer:
  - I can query it to find out what my assets are
  - I can compare the network against it to find out if the network and the policy agree.
- Now I can see my network traffic in a way that is meaningful to my network and my business

Contrasting Industry Approaches

SECURIFY

Better Approach	*Traditional*
• At the assets	• At the Perimeter
• Unified app and network	• Separate app and network
• Focus on the right things that should happen	• Focus on bad things that can happen.
• Policy scales easily	• Hard to scale & manage
• Looking for Acceptable behavior (finite problem) – *All other* behavior is a automatically violation of the policy	• Looking for known signatures and viruses – *Infinite* number of unknown signatures & viruses
• Highlight when an asset is compromised	• Detects an attack, not a compromise
• 24x7 audited	• Periodically audited
• Customer is in control	• Security Product vendor is in control

The Wireless Revolution and Security

SECURIFY℠

- The scale of the invasion of the wireless device
- Effects on the infrastructure
- Effects on the consumer
- Effects on the society, businesses, government
- International issues
- Increases the need for better security measures
- Complicates all aspects of the infrastructure security

The Wireless Device and the Critical Infrastructure

SECURIFY

- Number of devices, applications and connections will make the security issue grow exponentially
- New medium for connecting devices to the Internet introduce new vulnerabilities
- The level of the security of the infrastructure depends on the number of possible connections between people, devices, computers, …
- New interactions between machines also introduce new vulnerabilities
- The technical limitations of wireless devices limits possible security functionality and could drive the industry to overlook important issues

Issues with Consumers

SECURIFY℠

- Consumer trust in the establishment!
- Convenience always wins – the industry should make the trust work
- Privacy issues are harder to track with higher connectivity

Changes to the Society

- Expectation of everyone to get things faster without affecting the trust!
- Privacy issues with more available data
- Difficult to understand the complex issues with who owns the data and where is it?

Businesses are Affected Too

SECURIFY℠

- Individuals having access to critical information outside the “traditional boundaries”
- Extending the security perimeter to many more devices with limited capabilities
- Confidential information, intellectual property issues
- Changes the magnitude of a “hack”

Law Enforcement and the Wireless World

SECURIFY℠

- Good and bad news!!!
  - Locations easier to determine, more connectivity
- Need more technologies to “filter and understand” the ever-expanding amount of information
- Peer-to-peer issues!

International Issues

- Wireless devices greatly enhances the capability of communicating beyond country borders
- An order of magnitude harder than the Internet wave in terms of complexity of management

Summary

- **Network and application security management must change**
  - **Need to control IP addresses**
- **Security risk must be managed based on the business requirements through a specific policy**
  - **SV enables you to explicitly define what machines should be accessing the network and what those machines should be doing**
    - Helps you deal with unauthorized access and incorrect use of information assets
- **Improved security management measures are needed today**
  - Tight control of configuration and management
  - Visibility of all traffic behavior

Contact Information

SECURIFY

Peter Harter

SVP Business Development & Public Policy

Securify, Inc.

http://www.securify.com

peter@securify.com

+01.650.812.9400 ext. 4186 office

+01.917.640.2016 mobile