CS 361S

Network Security and Privacy

Vitaly Shmatikov

http://www.cs.utexas.edu/~shmat/courses/cs361s/

Course Personnel

- Instructor: Vitaly Shmatikov
  - Office: GDC 6.812
  - Office hours: Tuesday, 1-2pm
  - Open door policy – don't hesitate to stop by!
- TA: Oliver Jensen
  - Office: GDC 6.818A
  - Office hours: Wednesday, 11am-12n
- Watch the course website
  - Assignments, reading materials, lecture notes

Prerequisites

- Required: working knowledge of C and JavaScript
  - The first project is about Web security
  - The second involves writing buffer overflow attacks in C
    - You must have detailed understanding of x86 architecture, stack layout, calling conventions, etc.
- Recommended: Introduction to Computer Security; Cryptography; Computer Networks; Compilers and/or Operating Systems
  - Not much overlap with this course, but will help gain deeper understanding of security mechanisms and where they fit in the big picture

Course Logistics

- Lectures
  - Tuesday, Thursday 11a-12:30p
- Three homeworks (30% of the grade)
- Two projects (10 + 15% of the grade)
  - A fair bit of C coding and PHP/JavaScript hacking
  - Can be done in teams of 2 students
  - Security is a contact sport!
- Midterm (20% of the grade)
- Final (25% of the grade)
- UTCS Code of Conduct will be strictly enforced

No make-up or substitute exams!

If you are not sure you will be able to take the exams in class on the assigned dates, **do not take this course!**

Late Submission Policy

- Each take-home assignment is due in class at 11am on the due date
  - 5 take-home assignments (3 homeworks, 2 projects)
- You have 3 late days to use any way you want
  - You can submit one assignment 3 days late, 3 assignments 1 day late, etc.
  - After you use up your days, you get 0 points for each late assignment
  - Partial days are rounded up to the next full day

Course Materials

- Textbook:

  Kaufman, Perlman, Speciner. “Network Security”
  - Lectures will not follow the textbook
  - Lectures will focus on “big-picture” principles and ideas of network attack and defense
  - Attend lectures! Lectures will cover some material that is not in the textbook – and you will be tested on it!
- Occasional assigned readings
  - Start reading “Smashing the Stack For Fun and Profit” by Aleph One (from Phrack hacker magazine)
  - Understanding it will be essential for your project

Other Helpful Books

- Ross Anderson's "Security Engineering"
  - Focuses on design principles for secure systems
  - Wide range of entertaining examples: banking, nuclear command and control, burglar alarms
- "The Shellcoder's Handbook"
  - Practical how-to manual for hacking attacks
  - Not a required text, but you may find it useful for the buffer overflow project
- Kevin Mitnick's "The Art of Intrusion"
  - Real-world hacking stories
  - Good illustration for many concepts in this course

Main Themes of the Course

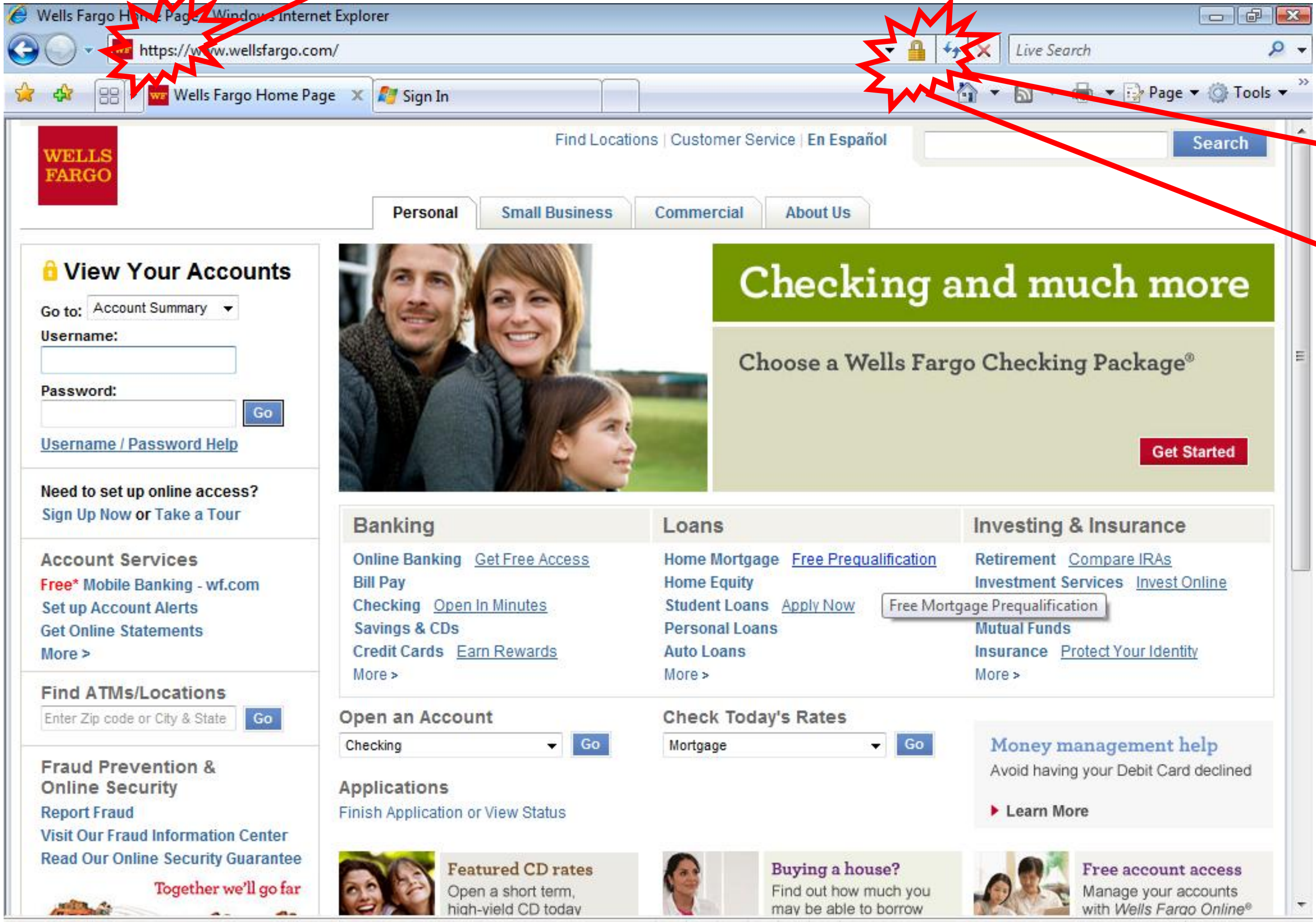
- Vulnerabilities of networked software
  - Worms and botnets, denial of service, attacks on Web applications, attacks on infrastructure
- Defensive technologies
  - Protection of information in transit: cryptography, application- and transport-layer security protocols
  - Protection of networked software: memory integrity, firewalls, antivirus tools, intrusion detection
- Study a few deployed protocols in detail: from design principles to implementation details
  - Kerberos, SSL/TLS, IPsec (if time permits)

What This Course is Not About

- Not a comprehensive course on computer security
- Not a course on ethical, legal, or economic issues
  - No file sharing, DMCA, piracy, free speech issues
  - No surveillance
- Only a cursory overview of cryptography
  - Take CS 346 for deeper understanding
- Only some issues in systems security
  - Very little about OS security, secure hardware, physical security, security of embedded devices…

Motivation

https://



Wells Fargo Home Page - Windows Internet Explorer

https://www.wellsfargo.com/

Live Search

Wells Fargo Home Page

Sign In

Page ▾ Tools ▾

WELLS FARGO

Find Locations | Customer Service | En Español

Search

Personal | Small Business | Commercial | About Us

View Your Accounts

Go to: Account Summary

Username:

Password:

Go

Username / Password Help

Need to set up online access?

Sign Up Now or Take a Tour

Account Services

Free* Mobile Banking - wf.com

Set up Account Alerts

Get Online Statements

More >

Find ATMs/Locations

Enter Zip code or City & State

Go

Fraud Prevention & Online Security

Report Fraud

Visit Our Fraud Information Center

Read Our Online Security Guarantee

Together we'll go far

Checking and much more

Choose a Wells Fargo Checking Package®

Get Started

Banking

Online Banking Get Free Access

Bill Pay

Checking Open In Minutes

Savings & CDs

Credit Cards Earn Rewards

More >

Loans

Home Mortgage Free Prequalification

Home Equity

Student Loans Apply Now

Personal Loans

Auto Loans

More >

Free Mortgage Prequalification

Investing & Insurance

Retirement Compare IRAs

Investment Services Invest Online

Mutual Funds

Insurance Protect Your Identity

More >

Open an Account

Checking

Go

Check Today's Rates

Mortgage

Go

Money management help

Avoid having your Debit Card declined

Learn More

Applications

Finish Application or View Status

Featured CD rates

Open a short term, high-yield CD today

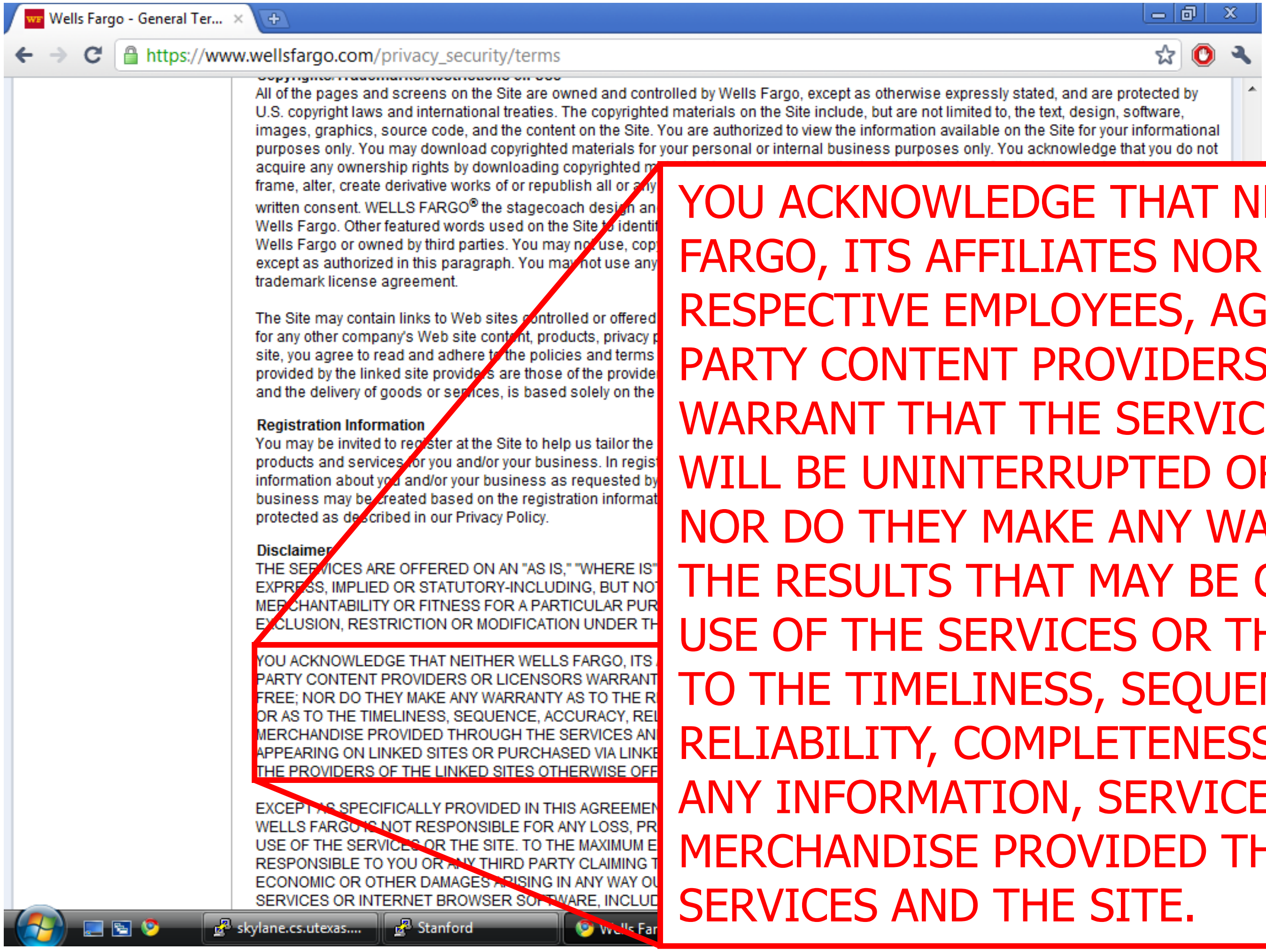
Buying a house?

Find out how much you may be able to borrow

Free account access

Manage your accounts with Wells Fargo Online®

Excerpt From “General Terms of Use”


Wells Fargo - General Ter...
https://www.wellsfargo.com/privacy_security/terms
skylane.cs.utexas....
Stanford
Wells Far

All of the pages and screens on the Site are owned and controlled by Wells Fargo, except as otherwise expressly stated, and are protected by
U.S. copyright laws and international treaties. The copyrighted materials on the Site include, but are not limited to, the text, design, software,
images, graphics, source code, and the content on the Site. You are authorized to view the information available on the Site for your informational
purposes only. You may download copyrighted materials for your personal or internal business purposes only. You acknowledge that you do not
acquire any ownership rights by downloading copyrighted m
frame, alter, create derivative works of or republish all or any
written consent. WELLS FARGO® the stagecoach design an
Wells Fargo. Other featured words used on the Site to identi
Wells Fargo or owned by third parties. You may not use, cop
except as authorized in this paragraph. You may not use any
trademark license agreement.

The Site may contain links to Web sites controlled or offered
for any other company's Web site content, products, privacy p
site, you agree to read and adhere to the policies and terms
provided by the linked site providers are those of the provide
and the delivery of goods or services, is based solely on the

Registration Information
You may be invited to register at the Site to help us tailor the
products and services for you and/or your business. In regis
information about you and/or your business as requested by
business may be created based on the registration informat
protected as described in our Privacy Policy.

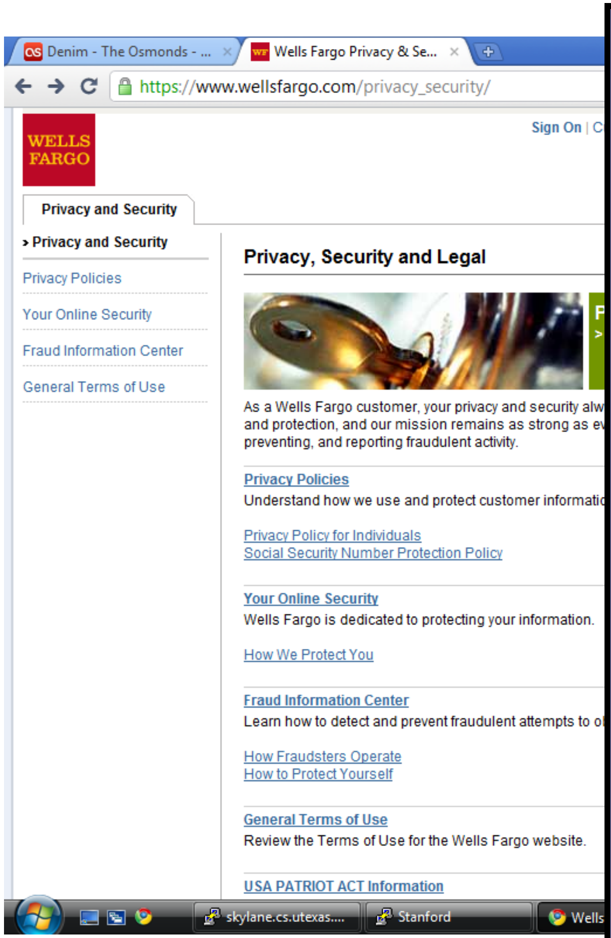
Disclaimer
THE SERVICES ARE OFFERED ON AN "AS IS," "WHERE IS"
EXPRESS, IMPLIED OR STATUTORY-INCLUDING, BUT NOT
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PUR
EXCLUSION, RESTRICTION OR MODIFICATION UNDER TH

YOU ACKNOWLEDGE THAT NEITHER WELLS FARGO, ITS A
PARTY CONTENT PROVIDERS OR LICENSORS WARRANT
FREE; NOR DO THEY MAKE ANY WARRANTY AS TO THE R
OR AS TO THE TIMELINESS, SEQUENCE, ACCURACY, REL
MERCHANDISE PROVIDED THROUGH THE SERVICES AN
APPEARING ON LINKED SITES OR PURCHASED VIA LINKE
THE PROVIDERS OF THE LINKED SITES OTHERWISE OFF

EXCEPT AS SPECIFICALLY PROVIDED IN THIS AGREEMEN
WELLS FARGO IS NOT RESPONSIBLE FOR ANY LOSS, PR
USE OF THE SERVICES OR THE SITE. TO THE MAXIMUM E
RESPONSIBLE TO YOU OR ANY THIRD PARTY CLAIMING T
ECONOMIC OR OTHER DAMAGES ARISING IN ANY WAY OU
SERVICES OR INTERNET BROWSER SOFTWARE, INCLUD

YOU ACKNOWLEDGE THAT NEITHER WELLS FARGO, ITS AFFILIATES NOR ANY OF THEIR RESPECTIVE EMPLOYEES, AGENTS, THIRD PARTY CONTENT PROVIDERS OR LICENSORS WARRANT THAT THE SERVICES OR THE SITE WILL BE UNINTERRUPTED OR ERROR FREE; NOR DO THEY MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES OR THE SITE, OR AS TO THE TIMELINESS, SEQUENCE, ACCURACY, RELIABILITY, COMPLETENESS OR CONTENT OF ANY INFORMATION, SERVICE, OR MERCHANDISE PROVIDED THROUGH THE SERVICES AND THE SITE.

"Privacy, Security and Legal"



Privacy, Security and Legal

As a Wells Fargo customer, your privacy and security alw
and protection, and our mission remains as strong as ev
preventing, and reporting fraudulent activity.

Privacy Policies
Understand how we use and protect customer informatio

Privacy Policy for Individuals
Social Security Number Protection Policy

Your Online Security
Wells Fargo is dedicated to protecting your information.

How We Protect You

Fraud Information Center
Learn how to detect and prevent fraudulent attempts to o

How Fraudsters Operate
How to Protect Yourself

General Terms of Use
Review the Terms of Use for the Wells Fargo website.

USA PATRIOT ACT Information

"As a Wells Fargo customer, your privacy and security always come first."

- Privacy policies
  - Privacy policy for individuals
  - Online privacy policy
  - Social Security Number protection policy
  - International privacy policies
- Your online security
  - How we protect you
  - Online security guarantee
- Fraud information center
  - How fraudsters operate
  - How to protect yourself
- USA PATRIOT ACT information

What Do You Think?

What do you think should be included in “privacy and security” for an e-commerce website?

?

Desirable Security Properties

- Authenticity
- Confidentiality
- Integrity
- Availability
- Accountability and non-repudiation
- Access control
- Privacy of collected information

…

Syllabus (1): Security Mechanisms

- Basics of cryptography
  - Symmetric and public-key encryption, certificates, cryptographic hash functions, pseudo-random generators
- Authentication and key establishment
  - Case study: Kerberos
- Web security
  - Case study: SSL/TLS
- IP security (if time permits)
  - Case study: IPsec protocol suite

Syllabus (2): Attacks and Defenses

- Web attacks
  - Cross-site scripting and request forgery, SQL injection
- Network attacks
  - Worms, viruses, botnets
  - Spam, phishing, denial of service
  - Attacks on routing and DNS infrastructure
- Buffer overflow / memory corruption attacks
- Defense tools
  - Firewalls, antivirus, intrusion detection systems
- Wireless security

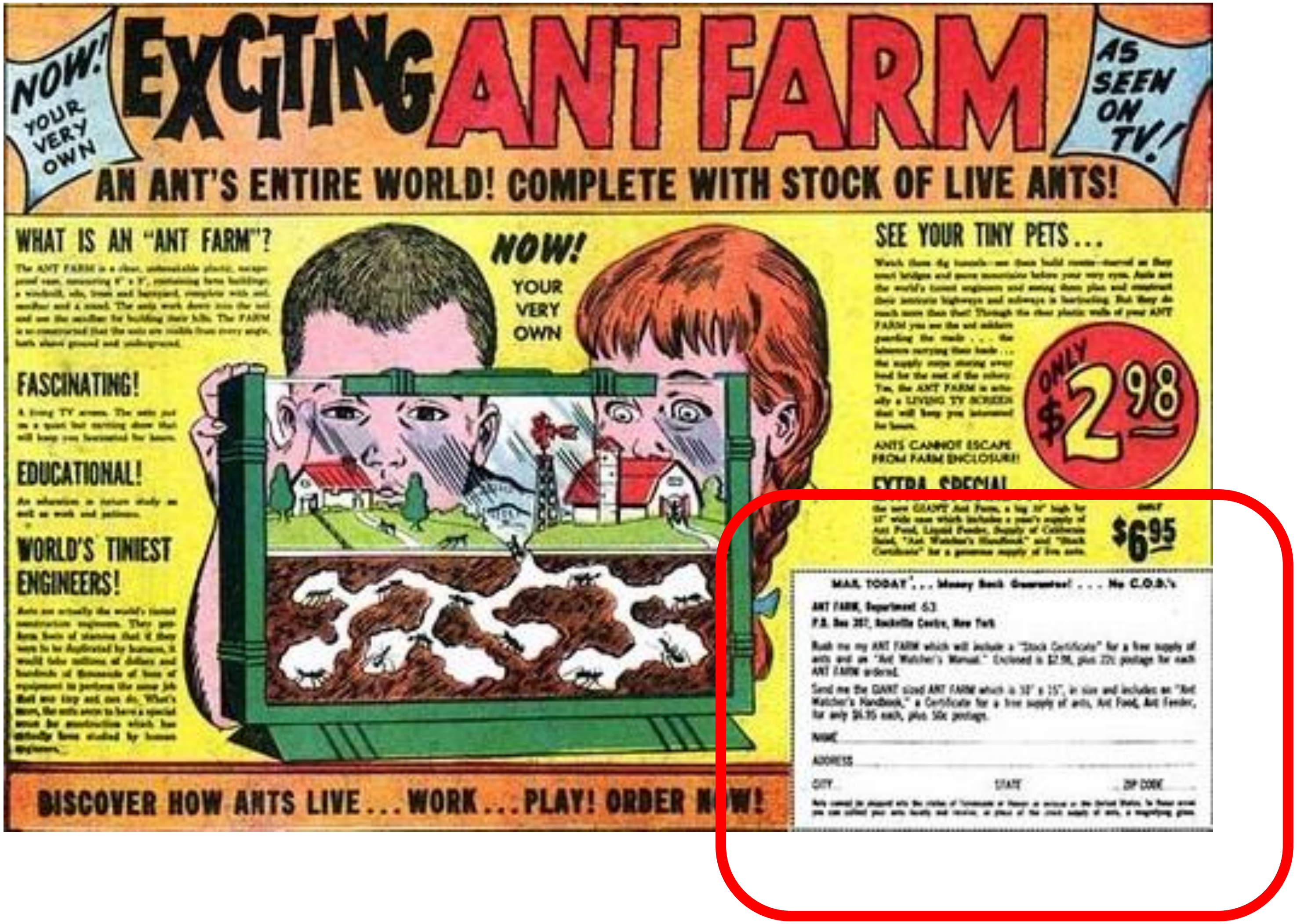
Peek at the Dark Side

The <u>only</u> reason we will be learning about attack techniques is to build better defenses

<u>Don’t even think about using this knowledge to attack anyone</u>

A Security Engineer’s Mindset

[Bruce Schneier]



AN ANT'S ENTIRE WORLD! COMPLETE WITH STOCK OF LIVE ANTS!

WHAT IS AN "ANT FARM"?

The ANT FARM is a clear, unbreakable plastic, escape-proof case, measuring 6" x 9", containing farm buildings, a windmill, silo, trees and barnyard, complete with soil, [illegible] and a stand. The ants work down into the soil and use the [illegible] for building their hills. The FARM is so constructed that the ants are visible from every angle, both above ground and underground.

FASCINATING!

A living TV screen. The ants put on a quiet but exciting show that will keep you fascinated for hours.

EDUCATIONAL!

An education in nature study as well as work and patience.

WORLD'S TINIEST ENGINEERS!

Ants are actually the world's tiniest construction engineers. They perform feats of stamina that if they were to be duplicated by humans, it would take millions of dollars and hundreds of thousands of tons of equipment to perform the same job that one tiny ant can do. What's more, the ants seem to have a special sense for construction which has officially been studied by human engineers.

SEE YOUR TINY PETS...

Watch them dig tunnels—see them build rooms—marvel as they erect bridges and move mountains before your very eyes. Ants are the world's tiniest engineers and seeing them plan and construct their intricate highways and subways is fascinating. But they do much more than that! Through the clear plastic walls of your ANT FARM you see the ant soldiers guarding the roads . . . the laborers carrying their loads . . . the supply corps storing away food for the rest of the colony. Yes, the ANT FARM is actually a LIVING TV SCREEN that will keep you interested for hours.

ONLY $2.98

ANTS CANNOT ESCAPE FROM FARM ENCLOSURE!

EXTRA SPECIAL

the new GIANT Ant Farm, a big 10" high by 15" wide case which includes a year's supply of Ant Food, Liquid Feeder, Supply of California Sand, "Ant Watcher's Handbook" and "Stock Certificate" for a generous supply of live ants.

ONLY $6.95

MAIL TODAY!... Money Back Guarantee! . . . No C.O.D.'s

ANT FARM, Department 63
P.O. Box 357, Rockville Centre, New York

Rush me my ANT FARM which will include a "Stock Certificate" for a free supply of ants and an "Ant Watcher's Manual." Enclosed is $2.98, plus 25¢ postage for each ANT FARM ordered.

Send me the GIANT sized ANT FARM which is 10" x 15", in size and includes an "Ant Watcher's Handbook," a Certificate for a free supply of ants, Ant Food, Ant Feeder, for only $6.95 each, plus 50¢ postage.

NAME

ADDRESS

CITY STATE ZIP CODE

Ants cannot be shipped into the states of [illegible] or [illegible] or anyplace outside the United States. In these areas you can collect your ants locally and receive, in place of the stock supply of ants, a magnifying glass.

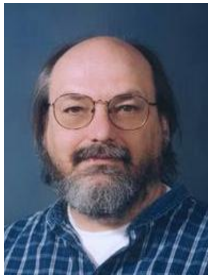
DISCOVER HOW ANTS LIVE...WORK...PLAY! ORDER NOW!

Ken Thompson

ACM Turing Award, 1983

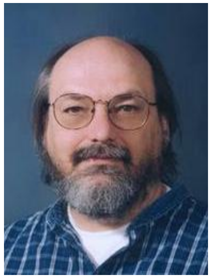
“Reflections on Trusting Trust”

http://www.acm.org/classics/sep95



- What code can we trust?
- Consider "login" or "su" in Unix
  - Is Ubuntu binary reliable? RedHat?
  - Does it send your password to someone?
  - Does it have backdoor for a “special” remote user?
- Can't trust the binary, so check source code or write your own, recompile
- Does this solve problem?

“Reflections on Trusting Trust”

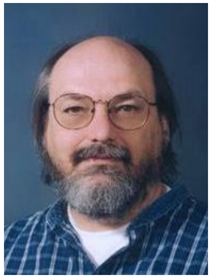


http://www.acm.org/classics/sep95

- Who wrote the compiler?
- Compiler looks for source code that looks the login process, inserts backdoor into it
- Ok, inspect the source code of the compiler… Looks good? Recompile the compiler!
- Does this solve the problem?

“Reflections on Trusting Trust”

http://www.acm.org/classics/sep95

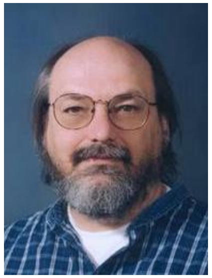


- The compiler is written in C …

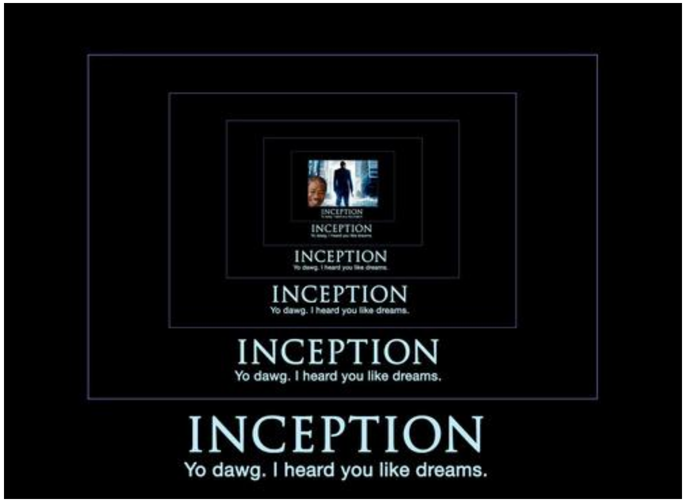
```
compiler(S) {
    if (match(S, "login-pattern")) {
        compile (login-backdoor)
        return
    }
    if (match(S, "compiler-pattern")) {
        compile (compiler-backdoor)
        return
    }
    …. /* compile as usual */
}
```

“Reflections on Trusting Trust”

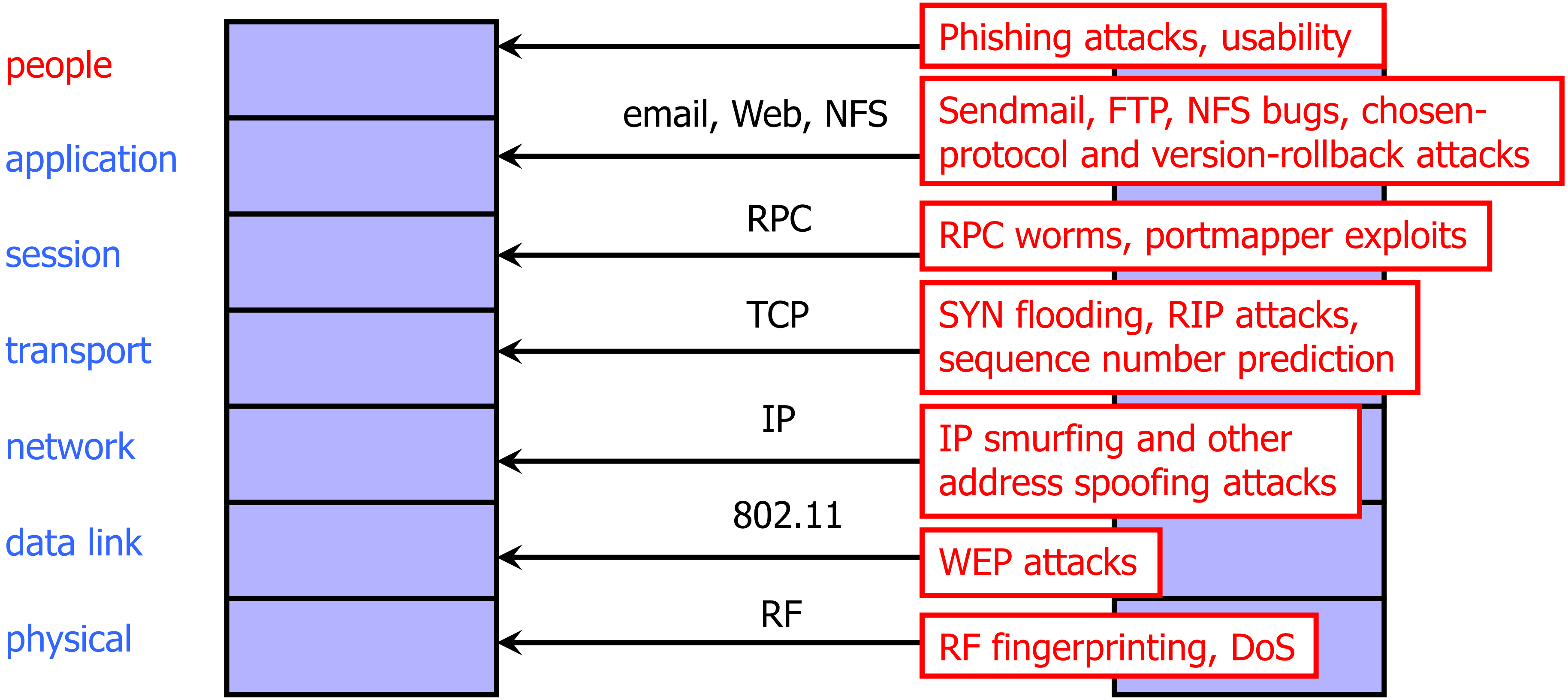
[redacted] http://www.acm.org/classics/sep95



“The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.)”


INCEPTION
Yo dawg. I heard you like dreams.
INCEPTION
Yo dawg. I heard you like dreams.
INCEPTION
Yo dawg. I heard you like dreams.
INCEPTION
Yo dawg. I heard you like dreams.
INCEPTION
INCEPTION

Network Stack



Phishing attacks, usability

Sendmail, FTP, NFS bugs, chosen-protocol and version-rollback attacks

RPC worms, portmapper exploits

SYN flooding, RIP attacks, sequence number prediction

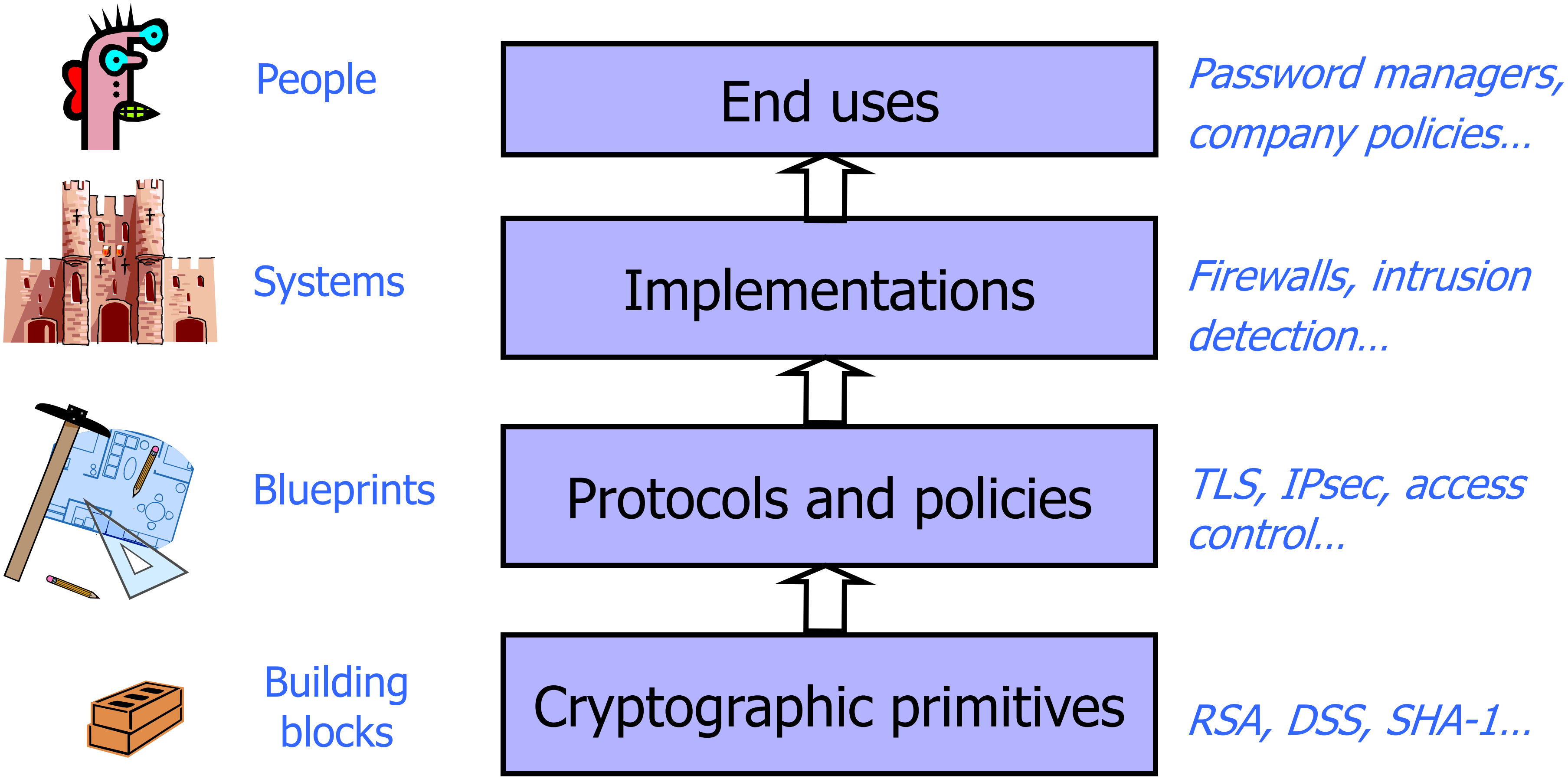
IP smurfing and other address spoofing attacks

WEP attacks

RF fingerprinting, DoS

Only as secure as the <u>single</u> weakest layer…
… or interconnection between the layers

Network Defenses



People

End uses

Password managers, company policies…

Systems

Implementations

Firewalls, intrusion detection…

Blueprints

Protocols and policies

TLS, IPsec, access control…

Building blocks

Cryptographic primitives

RSA, DSS, SHA-1…

<u>All</u> defense mechanisms must work correctly and securely

Correctness versus Security

- System correctness:
  system satisfies specification
  - For reasonable input, get reasonable output
- System security:
  system properties preserved in face of attack
  - For unreasonable input, output not completely disastrous
- Main difference: active interference from adversary
- Modular design may increase vulnerability …
  - Abstraction is difficult to achieve in security: what if the adversary operates below your level of abstraction?
- … but also increase security (small TCB)

What Drives the Attackers?

- Put up a fake financial website, collect users' logins and passwords, empty out their accounts
- Insert a hidden program into unsuspecting users' computers, use it to spread spam or for espionage
- Subvert copy protection for music, video, games
- Stage denial of service attacks on websites, extort money
- Wreak havoc, achieve fame and glory in the blackhat community

Marketplace for Vulnerabilities

- Option 1: bug bounty programs
  - Google: up to $3133.7 in 2010, now up to $20K per bug
  - Facebook: up to $20K per bug
  - Microsoft: up to $150K per bug
  - Pwn2Own competition: $10-15K
- Option 2: vulnerability brokers
  - ZDI, iDefense: $2-25K
- Option 3: gray and black markets
  - Up to $100-250K reported (hard to verify)
  - A zero-day against iOS sold for $500K (allegedly)

It’s a Business

- Several companies specialize in finding and selling exploits
  - ReVuln, Vupen, Netragard, Exodus Intelligence
  - The average flaw sells for $35-160K
  - $100K+ annual subscription fees
- Nation-state buyers
  - “Israel, Britain, Russia, India and Brazil are some of the biggest spenders. North Korea is in the market, as are some Middle Eastern intelligence services. Countries in the Asian Pacific, including Malaysia and Singapore, are buying, too” -- NY Times (Jul 2013)

Marketplace for Stolen Data

[Dell SecureWorks, 2013]

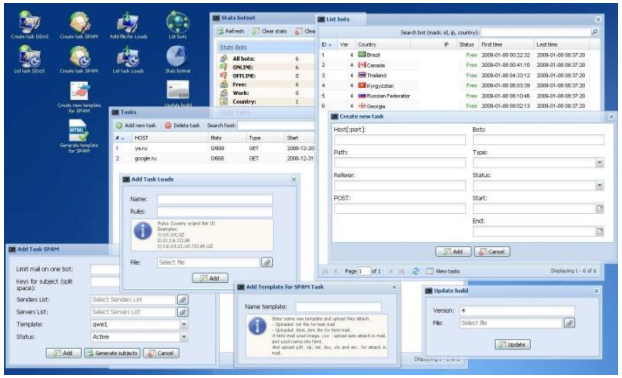
- Single credit card number: $4-15
- Single card with magnetic track data: $12-30
- “Fullz”: $25-40
  - Full name, address, phone, email addresses (with passwords), date of birth, SSN, bank account and routing numbers, online banking credentials, credit cards with magnetic track data and PINs
- Online credentials for a bank account with $70-150K balance: under $300

Prices dropped since 2011, indicating supply glut

Marketplace for Victims

[Trend Micro, “Russian Underground 101”, 2012]

- Pay-per-install on compromised machines
  - US: $100-150 / 1000 downloads, “global mix”: $12-15
  - Can be used to send spam, stage denial of service attacks, perform click fraud, host scam websites
- Botnets for rent
  - DDoS: $10/hour or $150/week
  - Spam: from $10/1,000,000 emails



Stats botnet

Refresh | Clear stats | Clea

Stats Bots

All bots:	6
ONLINE:	6
OFFLINE:	0
Free:	6
Work:	0
Country:	1

List bots

Search bot (mask: id, ip, country):

ID	Ver	Country	IP	Status	First time	Last time
1	4	Brazil		Free	2009-01-08 00:22:32	2009-01-08 08:37:20
2	4	Canada		Free	2009-01-08 00:41:10	2009-01-08 08:37:20
3	4	Thailand		Free	2009-01-08 04:33:12	2009-01-08 08:37:20
4	4	Kyrgyzstan		Free	2009-01-08 06:03:39	2009-01-08 08:37:20
5	4	Russian Federation		Free	2009-01-08 06:10:46	2009-01-08 08:37:20
6	4	Georgia		Free	2009-01-08 08:02:13	2009-01-08 08:37:20

Page 1 of 1 | View tasks | Displaying 1 - 6 of 6

Tasks

Add new task | Delete task | Search host:

#	HOST	Bots	Type	Start
1	ya.ru	0/999	GET	2008-12-20
2	google.ru	0/666	GET	2008-12-31

Create new task

Host[:port]:
Bots:
Path:
Type:
Referer:
Status:
POST:
Start:
End:

Add | Cancel

Add Task Loads

Name:
Rules:

Rules: Country or/and Bot ID.
Examples:
1) US,UK,UZ
2) 22,3,9,122,98
3) 3,9,US,23,UK,133,98,UZ

File: Select file

Add

Add Task SPAM

Limit mail on one bot:
Keys for subject (split space):
Senders List: Select Senders List
Servers List: Select Servers List
Template: qwe1
Status: Active

Add | Generate subjects | Cancel

Add Template for SPAM Task

Name template:

Enter name new template and upload files attach.
- Uploaded .txt file for text mail
- Uploaded .html, .htm file for html mail.
If html mail used image, css - upload auto attach in mail and used name into html.
And upload pdf, zip, rar, doc, xls and etc. for attach in mail.

Update build

Version: 4
File: Select file

Update

- Tools and services
  - Basic Trojans ($3-10), Windows rootkits ($300), email, SMS, ICQ spamming tools ($30-50), botnet setup and support ($200/month, etc.)

Bad News

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems may be poorly understood
- Implementations are buggy
  - Buffer overflows are the "vulnerability of the decade"
  - Cross-site scripting and other Web attacks
- Networks are more open and accessible than ever
  - Increased exposure, easier to cover tracks
- Many attacks are not even technical in nature
  - Phishing, social engineering, etc.

Better News

- There are a lot of defense mechanisms
  - We’ll study some, but by no means all, in this course
- It’s important to understand their limitations
  - “If you think cryptography will solve your problem, then you don’t understand cryptography… and you don’t understand your problem”
  - Many security holes are based on misunderstanding
- Security awareness and user “buy-in” help
- Other important factors: usability and economics

Reading Assignment

- Review Kaufman, section 1.5
  - Primer on networking
- Start reading buffer overflow materials on the course website
  - “Smashing the Stack for Fun and Profit”
  - You will definitely need to understand it for the buffer overflow project