

The Internet as unstable medium

(as published on Security Focus, May 2000
by Roelof Temmingh @ SensePost)

This article is about exploiting Internet users' ignorance, the IT industry's race for information, and the hype around the IT industry.

Note: This article was written before the ILOVEYOU virus hit the world, and all of a sudden it seems very relevant. It has been slightly edited after the virus strike.

Introduction

The damage caused recently by the ILOVEYOU virus has once again raised awareness about the threat of content level attacks, especially in Microsoft environments. Poor Microsoft... The world just loves to hate them. And not without reason. But is it fair to lay all the blame on Microsoft's feet? Let's look at the Internet world the way it is today.

We are the generation of instant gratification and the Internet is our medium. Users have an ever-increasing hunger for information, cyber-offerings and interactive entertainment. They are force-fed gigabytes of data by information warehouses such as CNN, IMDB, Yahoo and the likes. Things happen at light-speed around here, and if you can't hang on, you loose out. Blink and you have missed another opportunity.

It's a dog eats dog world. Time to market is measured in hours and minutes and the first kid on the block is often the leader, even if he's not the biggest and strongest. We release products and service offerings before they exist in real life. You're not complete if you don't have an official web-site and company names are chosen according to .com namespace availability.

This culture has three distinct characteristics, all of which are impacting security today.

Firstly, the Internet culture is anonymous. We have free email, free web-space, free anonymisers, free remailers and free Unix shells. We can register domains online, with credit cards; we can set up DNS servers for no charge. Get your email for nothing, get your DNS for free. Cybercafes are open 24h a day and using them requires no identification. It is even possible to create totally fictitious services, companies, or corporations - offering services that don't exist. It's easy to be anonymous on the Internet.

Secondly, the culture is spoiled - always giving users exactly what they want. As the Internet is becomes mainstream, companies design software to be more and

more "user-friendly". Using the Internet has to be seamless, it has to be easy, and it has to require as little user interaction as possible. We really have to connect the panting user with his/her resource. It's an OK/Continue button clicking culture and the less the user understands of what's actually going on, the better. It would be very interesting to measure the average technical knowledge of Internet users over the past 10 years...

Thirdly, the Internet is about hype. Chain letters from Nokia and Ericsson claiming that you could get a free WAP-enabled cell phone flood Internet links everyday. Users believe that Bill Gates will pay them each \$1000 if they forward messages to everyone in their address book telling them about W2K. Vaporware and vapor-offerings. Current flavor-of-the-month is e-commerce. We're building EFTs, transaction servers, and super strong encryption systems all in the name of providing E-commerce solutions to the world. And everyone wants in.

It's this culture that's made Microsoft the most successful software company in the world. Microsoft gives people what they want. What people want is software that is simple and easy to use and that masks the technical complexity. It's this requirement that creates security problems. If people don't understand how the technology works they'll never understand the security issues. There will always be bad people tricking dumb users into making their computers do things they shouldn't.

But there are other ways of abusing the Internet culture. Here's a recipe for tricking people into giving you money:

Examples

Example 1: The South African lottery

A concept that lives IRL, but not on the Internet (yet).

Note 1:

The South African national lottery is a very "happening/current" event. It has been running for 2 months and everyone is buying. There are daily TV and newspaper ads.

Note 2:

A few South African banks have implemented a "direct payment" method on their Internet-banking sites, allowing users to transfer money from their accounts into any other account at any other bank, all online. The banks use only server side certificates and users are authenticated using an account number and a PIN. Security thus hinges on an account number and a PIN code. A ticking time bomb...

How to:

1. Register "salottery.com". Register.com also provides web-hosting and DNS hosting. Assign an IP number to www.salottery.com

2. Build a website

The online SA national lottery website:

- Sponsored by Telkom SA using CyberTrade (tm) as secure backend.
- Endorsed by all the major SA banks (Nedbank, StandardBank, and ABSA).
- As we don't need expensive lottery ticket printing equipment, on-line lottery tickets are 50c cheaper than "offline" tickets.
- Lottery tickets appear as screen (with barcode etc) that can be printed.
- Can also be saved as a file that can be printed later. SALB (South African Lottery Board) approved. [This body does not exist] Audited by major auditing house (KPMG or the likes). Separate link (about security) that explains in VERY technical terms how SSL v3 works [although no SSL is used]
- Add banner ads from sponsors - e.g. "Telkom - we are the future".
- There is a 'pay page' allowing users to enter their bank account number and PINs - for 'direct' banking payments

3. Spread the rumor

Spread the rumor of online lottery tickets to mailing lists, newsgroups and farmed *.za email addresses. (Hey, buy a CDROM containing email addresses and do a grep for ZA)

4. Collect credit card numbers and Internet-banking account number and PIN combinations.

What I'm doing here isn't a technical attack but the effect is the same. Read the intro again if you still don't get it...

This example can very easily be expanded. Forget the lottery. Register www.choose-a-bank-here-secure.co.za/com (add something like "secure" or "plus"). Copy the original bank's page to the new site, and spread the rumor the bank is launching an extended service. Collect account numbers and PINs. Or 'design' a great new product and sell it on the web. It will be months before realize they've been had:

Example 2: The Sony MP3walkabout

A product that totally does not exist

How to:

1. Register

Register sonywalkabout.com at www.register.com. Register.com also provides web hosting and DNS hosting. Assign an IP number to www.sonywalkabout.com.

2. Build a website

Get a really good idea of the "product":

- MP3 CDROM device - it uses normal data CDROMs that contain MP3s
- Lithium Ion batteries gives 12h playtime and are rechargeable
- Ripping software bundled with hardware.
- ShockAssist (tm) firmware and 24x over sampling ensure no data loss.
- MiniDisc version coming out soon..
- Add the following to the page:
 - Complete technical specifications online
 - White paper on MP3 compression technology
 - Reviews by mp3.com and bleeding edge columnists
- Use Sony logo and color scheme...make it look real and official.
- Add online ordering of product:
- Accept MasterCard, Visa and others.
- First 100 order requests win free device.

3. Spread the rumor

Spread a rumor about the page. Write to slashdot, mp3.com and mailing lists. Contact several techno/audio-freaks in the industry that write for online audio, mp3 magazines. "Leak" news of the product to newsgroups.

4. Collect credit card numbers.

Example 1 & 2 Note: this system is totally "off-feed" - e.g. no feedback is given to the user. There is no way to verify that this site is a hoax, other than contacting governing bodies, or the site being taken down.

Some people might say that if I did any of the above activities I would be rounded up in no time, and spend a significant time in jail. However, precautions could be taken. If followed very closely, one should retain total anonymity.

- Every single bit of data is sent and received from cyber cafés
- All information submitted (real name, address etc) are factious
- All sessions are executed from different cyber cafés.
- Where possible, anonymizers are used to hide physical location.
- Where real information (such as credit card information) are used, the information is stolen.
- Do not discuss methods and actions with ANYONE - no silly hacker handles are left anywhere.

Solutions

So how do we safeguard against these types of "social-technological" attacks? The problem is complex and can't be solved simply by throwing more and more technology at it. What's required is a paradigm shift – probably uncomfortable but essential for a long-term stable Internet economy.

Here are some suggestions:

Education of users

The advanced, know-the-technology person would not be fooled by the examples here. When ATMs were first introduced, many people were fooled into giving their cards and PIN numbers to complete strangers. Soon enough the "communal conscience" grew wary of strangers offering "help". The problem with the Internet is that we are all part of the "first generation" of e-commerce users. Internet commerce is a new thing - even the World Wide Web is merely 10 years old! Many people accept anything offered to them over the Internet as OK the same way they believe 'the computer is always right'. Users need to be educated not to trust everything they're offered. This is largely the responsibility of software houses and service providers.

Fix the software

Software should be written to be more security-aware. Early versions of IE4 did not connect to websites if the server certificate or the CA certificate could not be verified. Why was it changed? It was changed because too many users complained that they couldn't connect to ill-configured sites. By enforcing the verification of server certificates, CA certificates and CA-chains, we not only protect the user, we force site builders and administrators to implement SSL in the correct way. Today's software provides too many possibilities for the user to screw themselves without knowing it.

Accountability

There's been talk of providing the all the Internet users with some kind of client ID. All IP packets originating from this user will be signed by the user's ID. The key-holder for such an ID could be smart card or USB token of some sort. An IPSec/IPv6 implementation where packets are not signed with a certificate belonging to the host, but to the user of the machine. I already hear the screams "what about privacy!". Will it be acceptable for the online community? Why do we require drivers to have a license when driving on the roads while users surf the information highways without any identification at all? There are other practical steps that can be taken. For example, in Malaysia one is required to provide positive identification before using Internet-

connected computers in cyber cafés. A raised level of accountability on the Internet will go a far way to discourage criminals using the Internet as their vehicle.

Conclusion

The weakest link will always be the user. We'll never be able to encrypt that post-it note on the screen. It is only by security awareness and user education that we make IT security technology work for us. Don't assume that a person who does stupid things in real life is not going to do them in an online world. Computers don't make people intelligent.

I can only hope that companies investing heavily in IT security and user awareness survive and those that don't go under. In a Darwinian world we might have the Internet as a stable electronic medium in 5 to 10 years.

Thanks & Shouts

As always, I like to thank Charl van der Walt for all his time he has put into this - my English sucks big time. Also thanks to all the people at SensePost for putting up with me all the time. And you thought all we do in South Africa is dodge the elephants...