]HackingTeam[

The Data Encryption Problem

A change in paradigm.

Collection of encrypted data.

Traditional approaches to decryption.

A different approach (to both).

Our experience with it.

Speaker: Daniele Milan

Senior Software Developer

HackingTeam Ltd.

Milano, Italy

Founded in 2003

Venture backed in 2007

Core business IT offensive security

Remote Control System (RCS)

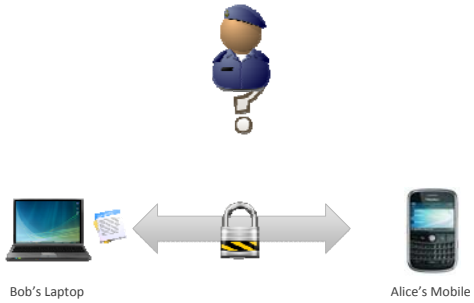
Let's begin.

Encryption.

Hiding information.

Common scenario.

]HackingTeam[



]HackingTeam[

Traditional lawful interception.

Any other channel you can tap.

]HackingTeam[

Encrypted data.

We don't care about the rest.

]HackingTeam[

We don't have the key.

]HackingTeam[

We don't know anything about the algorithm.

]HackingTeam[

Potentially thousands of encrypted communications per day.

]HackingTeam[

How can we decrypt that data?

]HackingTeam[

Bruteforcing is impratical.

Keyspace can be made vast with good passwords.

]HackingTeam[

Cryptanalysis.

Accessing encrypted information without the secret key.

]HackingTeam[

Algorithms in common use are a few.

RSA.

AES.

]HackingTeam[

SSL is the most common protocol.

]HackingTeam[

Peer reviewed, tested and sound.

Some (highly) theoretical attacks.

Not usable in real cases.

]HackingTeam[

You're not going to spend much time on breaking AES or RSA, are you?

]HackingTeam[

We cannot guess the secret key.

We cannot break the algorithm.

]HackingTeam[

There must be another way.

]HackingTeam[

We forgot some players.

Bob and Alice.

]HackingTeam[

We are talking about modern communications.

Bob and Alice use devices to communicate.

Computers and smartphones.

]HackingTeam[

People and computers.

]HackingTeam[

The weakest link.

]HackingTeam[

You can trick people in doing what you want them to do.

Think about ads …

]HackingTeam[

You can evade computer security.

]HackingTeam[

A short “what if” game.

]HackingTeam[

What if …

I can install an “agent” on Bob’s computer?

]HackingTeam[

Contrary to common belief a manageable effort.

]HackingTeam[

Well, easier than breaking the math.

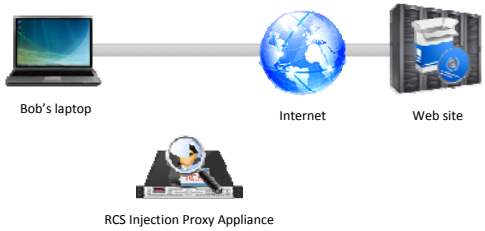
]HackingTeam[

As easy as sending an SMS.

]HackingTeam[

You can also play the hackers game.

]HackingTeam[



]HackingTeam[

Zero day exploits.

Turn documents into weapons.

]HackingTeam[

Don’t forget the people.

Social engineering.

Trick them.

Be creative.

]HackingTeam[

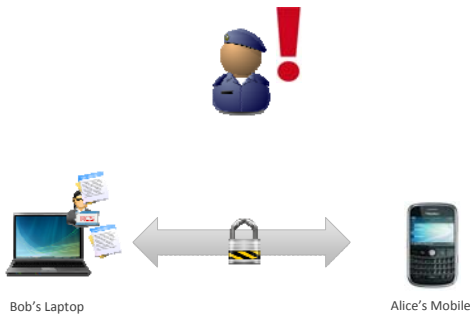
If you’re methodical

you can expect consistent results.

]HackingTeam[

Our software agent is installed on Bob’s laptop.

]HackingTeam[



]HackingTeam[

What if …

our agent is able to get the cleartext?

]HackingTeam[

The data encryption problem is no more.

]HackingTeam[

What if …

our agent is able to get the keys, too?

]HackingTeam[

Cleartext is my primary target.

But the keys open the realm.

]HackingTeam[

I can decrypt what I cannot take in cleartext.

]HackingTeam[

Complements traditional lawful interception.

]HackingTeam[

I can also impersonate someone.

Cryptographically sound.

]HackingTeam[

Breaking into devices is a manageable

one shot effort.

You can expect results.

]HackingTeam[

Let's forget about encryption.

]HackingTeam[

We talked about traditional lawful interception.

]HackingTeam[

Limited in range of action.

]HackingTeam[

Limited by country borders.

]HackingTeam[

With an agent, you get data from anywhere.

]HackingTeam[

Regardless of distance.

Protocols.

Laws.

Third party cooperation.

]HackingTeam[

There's more.

]HackingTeam[

The most interesting data never travels on the Internet.

]HackingTeam[

Contact list.

Agenda.

Documents & plans.

]HackingTeam[

The agent approach exposes you to a new series of problems.

You want guarantees.

]HackingTeam[

Antiviruses actively search for "hidden" software.

Our agent must be invisible.

]HackingTeam[

Our agent will face different scenarios.

You want it flexible and able to adapt itself.

]HackingTeam[

Prevent disclosure of your identity.

Our agent must communicate covertly.

]HackingTeam[

]HackingTeam[

Our experience with Remote Control System.

]HackingTeam[

Tactical solution.

]HackingTeam[

Police forces.

Intelligence agencies.

5 continents.

(estimated) thousands of targets.

]HackingTeam[

High success rate.

Positive feedbacks.

]HackingTeam[

Our core business.

]HackingTeam[

Let's sum up.

]HackingTeam[

Forget about encryption.

Intercept them anywhere.

Get what you usually miss.

]HackingTeam[

For more, please get in touch.

]HackingTeam[

Any idea?

We are listening.

]HackingTeam[

info@hackingteam.it

]HackingTeam[