Chaos to the Rescue

Strengthening IT Security

The chaos theory was discovered in the mathematics field and began to be observed in daily life during the second half of the 20th century. Chaos is a scientific theory that aims to explain or even give some predictability to complex systems. At first glance, the chaos theory resembles most mathematical discoveries—an interest solely of the mind. For example, imagine a researcher spending days staring at the sky to find some logic in the dissipation of clouds or a scientist counting the branches of a snowflake. One may question the importance of a dissipated cloud or the act of infinitely reproducing a tiny snowflake. Yet by using these oddities (chaotic systems), mathematicians find patterns, i.e., fully predictable mathematical models, named strange attractors.

The chaos theory also enabled the discovery of dimensions of space that are no longer whole, named fractals. For example, a broken line that is formed with four line segments of the same length is considered to be a fractal line of one-fourth (¼) dimension. These infinite replications of the same design are also found everywhere in natural phenomena, e.g., blood vessels, broccoli flowers and mountain ranges. Weather forecasting uses the chaos theory every day. Chaos processes are also used in economics, to improve room temperature, to understand aviation turbulence, to explain how brain cells increase and in IT cryptography.

Introducing chaotic processes in technology may help address security challenges. Without this, there will always be an issue in IT security.

By using the chaotic theorems that were deduced from a set of complex numbers, physicists arrived at two paradoxical findings:

- Some degree of uniformity and order can be found in apparently erratic and uncontrollable phenomena.
- A phenomenon that is very controllable and predictable, such as the trajectory of a planet around the sun, can become very unpredictable over a period of tens of millions of years.

The chaos theory concepts mentioned previously can be used to find optimal solutions to critical security problems in information systems such as identity theft and counterfeiting and make information systems more secure. This can be illustrated through the example of a new electronic identification card. This card integrates chaotic

Jean Jacques Raphael, CISA, CISM, ISO 27001 LI
Is a lead implementer of IT security at OctoSafes Inc. He is a gold ISACA® member and belongs to the Montreal (Quebec, Canada) Chapter.

Jean Claude Célestin
Manages practical work at the University of Ottawa (Canada).

Eric Romuald Djiethieu, FCNSP, ISO 27002 Foundation, ITIL v3
Is an IT security and telecommunication architect at Desjardins. He is also a cofounder of OctoSafes Inc.

© 2019 ISACA. All rights reserved. *www.isaca.org*

processes in all aspects of its operation and design. It accounts for erratic microcircuits cabling, defects in the physical structure and multifrequency variations.

The approach to finding these chaos-based security solutions is based on five hypotheses. The last two hypotheses are deduced from the first three:

1. A child born today can be identified and authenticated by a computer without using the child's name or a numerical identifier.
2. On a certain scale (e.g., micron [micrometer] or microsecond), it is impossible for two people or two objects to be exactly the same (e.g., identical twins, fingerprints, two sheets of paper in the same ream).
3. To become safer or even impenetrable, information systems must obey new laws and new logic (other than Boolean logic).
4. The computer can protect people by protecting itself.
5. It is now possible, based on the previous hypotheses, to design information systems with limited compatibility (i.e., it is impossible for two computers to communicate if there has not been some "physical" interaction [remotely or not] between these two systems).

> “TO BECOME SAFER OR EVEN IMPENETRABLE, INFORMATION SYSTEMS MUST OBEY NEW LAWS AND NEW LOGIC.”

Digitizing Chaos Enables a New Type of Cybernetics

Although scientists and technologists are trying many ways to change how information systems work, such as coding information in the same way that DNA is coded (four initial states) or applying quantum theory (quantum bits), the chaos theory is a more accurate way to resolve information system issues.

To strengthen and test the idea of digitalizing chaos to protect personal data and machines (e.g., PCs, planes and drones) from any accidental or malicious manipulation or to guarantee authenticity (e.g., for medicines, wines and perfumes), researchers designed a computer containing algorithms and chaos logic circuits that allow it to function according to the chaos theory. This computer is a polymer chip card with the dimensions of a credit card. The card stores the genetic, biometric and birth date data of a newborn child. This card will be an integral part of the life of its owner (from birth to death) and will help the owner to identify and authenticate his or her identity during certain crucial activities where the confidentiality, integrity and availability criteria are mandatory.

The computer system uses traditional Boolean logic and the Open Systems Interconnection (OSI) model[1]; these tools are used in millimetric scale and during microsecond time intervals. Because security is a matter of support, the computer's physical characteristics will also be used for security purposes. Every time the card communicates with an authentication server, physical contact is maintained. When the physical contact is suspended, the communication is canceled.

Chip Card Description

The chip is to be fabricated with a stable polymer that is inalterable and immutable by temperature or time. A refractory glass coating protects it from fire.

This familiar medium can become a complex system when subjected to a spatio-temporal analysis. It is impossible to use sight and touch to distinguish between chip cards. If the cards are scanned with a laser beam of a few microns in diameter, differences are revealed (proving the second hypothesis). The scan shows that the chip cards have bumps and hollows. In addition, the machine that inserts the chip on cards varies the chip placement. For example, the chip of card 1 is placed 10 microns from the right side of the card, the chip of card 2 is placed 11 microns from the right side of the card and the chip of card 3 is placed at 12 microns from the right side of the card. These slight variations, undetectable to the naked eye, strengthen the uniqueness of each card.

© 2019 ISACA. All rights reserved. *www.isaca.org*

The machine that produces these cards can further strengthen their uniqueness by registering their creation time. For example, if card 1 was created on 22 December 2018 at 2h: 35m: 00s: 01ms and card 2 was created on 22 December 2018 at 2h: 35m: 00s: 02ms, this millisecond difference is a key value—strengthening, in a definitive way, the uniqueness of each card.

The topology variations of each card are saved on a hard disk on the authentication server. This information is replicated in less than 24 hours on other servers spread over a radius of more than 100 km, ensuring a backup. If a card owner loses the card, the process is resumed based on the information contained on the authentication server and the immutable data of the card owner (date of birth, genetic and biometric data) are transferred to a new card. The information that was on the lost card is sent to another server and kept for a decade. The lost card is permanently unusable and destroyed if it appears again.

The genetic and biometric data of a newborn child are recorded and analyzed by an authentication server (AS) that stores information about the physical characteristics of the card, the child's genetic and biometric data, and date of birth to the nearest millisecond. This AS is the property of the government and should be replicated throughout some government offices, such as hospitals and embassies. The chip card communicates with this AS each time this child's identity must be authenticated. The biometric (fingerprint) and genetic (DNA) data are more than enough to authenticate the identity of the child, proving the first hypothesis. For reasons of legal responsibility, one must add the genetic and biometric data of the person responsible for the child (e.g., a parent or guardian). A name or a Social Security Number (SSN) must be added to the card, but this information would not allow someone to conduct a fraudulent transaction by posing as this person. Furthermore, the name and SSN of the person should be printed on the card because this is the only way of distinguishing the cards during mass data collection.

Chaos and Card Cybersecurity

Based on its theorems, the chaos theory reveals two findings of everyday life:

- It is possible from a finite or tiny space to reach an infinite outcome. For example, analysis shows that, under magnification, a snowflake always has six branches, and, on each of these branches, there are six smaller branches, which have six branches each, and so on. To observe as many branches as possible, the flake must be enlarged.
- It is often impossible to deterministically or randomly predict the outcome of a system. For example, it is impossible, based on the attraction of other planets or even the moon, to accurately predict the position of the earth with respect to the sun after 10 million years.

> “THE UNIQUENESS OF EACH TRANSACTION, ASSOCIATED WITH OTHER ENCRYPTION MECHANISMS, GUARANTEES THE INVIOLABILITY OF THE SYSTEM.”

To demonstrate the integration of chaos into cybersecurity, three example cards for users Jean, Claude and Eric are presented. These three cards were set to initialization in contact with the authentication server previously described. From this phase, the two machines can decide to communicate with each other using only well-defined frequency bands. For Jean, the analysis of the surface of the card and the transmission of data are completed using the following frequency bands in a random and nonrepetitive manner: 0 to 10 GHz, 50 to 70 GHz and 200 to 205 GHz. For Claude, the bands of 15 to 20 GHz, 40 to 60 GHz and 201 to 206 GHz are used. For Eric, the bands of 7 to 9 GHz, 80

© 2019 ISACA. All rights reserved. *www.isaca.org*

to 90 GHz and 205 to 305 GHz are used. These unique and unpredictable frequency variations are associated with other encrypted information—useful message (e.g., the amount that will be withdrawn, the bank name and the account number for an ATM transaction), time, latitude and longitude, biometric and genetic data, and physical characteristics of the card—and make any attempt by someone to find a pattern through the transactions impossible. Fraudulent attempted card transactions are rejected because the frequency used is prohibited for the card.

Like the snowflake whose number of observable branches depends on magnification, the physical structure of each card varies with each variation in frequency: The number of hollows (0) and bumps (1) vary because the scan frequency is, for example, 10 or 2.5 GHz. Only the card-authentication server system knows if the frequency that is used is allowed (proving the fourth hypothesis). The uniqueness of each transaction, associated with other encryption mechanisms, guarantees the inviolability of the system.

Because the genetic and biometric data are collected and analyzed on micron scales, they cannot be reproduced (proving the second hypothesis).The examination and storage of this phenomenal amount of information at these microscopic scales is possible due to the ability to save terabytes of data in smaller and smaller volumes.

Only the machine can identify these data or reject them (hypothesis 4) when anyone attempts to reproduce them. Any gap from the initial setup range (a few microns or microseconds) causes a rejection. To reproduce all the details, a person's sense abilities would need an average magnification of 1,000 times to be able to sense the information contained on a card. Due to the temporal dimension, it is impossible to reproduce the same data even using the same machine.

Another example demonstrates an extreme case—twin children with similar genetic and physical characteristics are born on the same day. Given that twin children are never born at the same time (to the nearest microsecond), their biometrics are different (to the nearest micron) and their birth certificates are printed on separate cards with distinct microscopic characteristics, it is impossible for one to pretend to be the other. The system can differentiate these two children because the communication between the AS and the card can unveil some microscopic details that differentiate these children. For example, only the card and the AS know how many microseconds elapsed between the printing of the two cards, how many hollows distinguish the second card from the first and how many micrometers differentiate the palm of each child. Those microscopic quantities will be undetectable and useless for people, but the two systems will be able to record them faithfully to prevent one child from assuming the identity of the other.

> “ONE OF THE WEAKNESSES OF BIOMETRIC-BASED SECURITY SYSTEMS IS THAT THE DATA COME FROM A SAMPLE THAT HAS BEEN DIGITALIZED.”

Addressing Weaknesses With Biometric Security

One of the weaknesses of biometric-based security systems is that the data come from a sample that has been digitalized (hypothesis 3). The case is different for the researchers' proposed system. The machine detects the relief (the surface roughness) of the card. Referring to layer 1 of the OSI model, the physical characteristics of the system (the card and the AS working together) are not limited only to electronic circulation or bandwidth. The machine's authentication server checks the initial roughness on a card to be certain that it is the same card that it analyzed initially and kept in memory. If the

© 2019 ISACA. All rights reserved. *www.isaca.org*

machine does not find the same topography, it refuses to authenticate the transaction. Because this roughness is digitized (e.g., 1 indicates a hump, 0 indicates a hollow), this information is part of the encryption process or the key to decoding useful information. This roughness does not exist in current systems. The decoding ability ensures the system's inviolability. Indeed, a man-in-the-middle exploit can still use a classic or quantum compiler, but it will never be able to determine if the bit that is isolated constitutes part of the physical medium of the information or represents a part of the information itself.

Self-Protection and Limited Compatibility

Hypotheses 4 and 5 relate to the card security because if the card has never been scanned by an authentication server, the card will never be able to communicate with this server in the future. The systems formed by the card and the server become compatible (hypothesis 5) only after an initial interaction. During this first contact, there are some communication protocols that both the AS and the card established. These recognition protocols happen without human intervention. This is possible through artificial intelligence algorithms.

Before authorizing any transaction, the server verifies if a card, with intrinsic physical characteristics and all the information stored on it, is part of its database. The slightest space-time discrepancy results in the rejection of the transaction. This interaction between the card and authentication server takes place at the level of the physical layer of the OSI model. Other communication and upper-layer transport protocols are only considered after this unavoidable physical contact. In addition to these explicit parameters, other patterns that are undetectable by human understanding and invisible to human senses are stored on the authentication server. For example, the Fibonacci series is found everywhere in natural phenomena.[2] The server may find this series in genetic and biometric data reproduced at micron scales. Therefore, these correspondences between the card and the server are interacting without the knowledge of any human intelligence, allowing the machine to protect itself (hypothesis 4) against any attempt of fraudulent reproduction. The self-protection and compatibility mechanisms make fraudulent access impossible.

> “ONE OF THE WEAKNESSES OF BIOMETRIC-BASED SECURITY SYSTEMS IS THAT THE DATA COME FROM A SAMPLE THAT HAS BEEN DIGITALIZED.”

Chaos Theory Cybersecurity Example

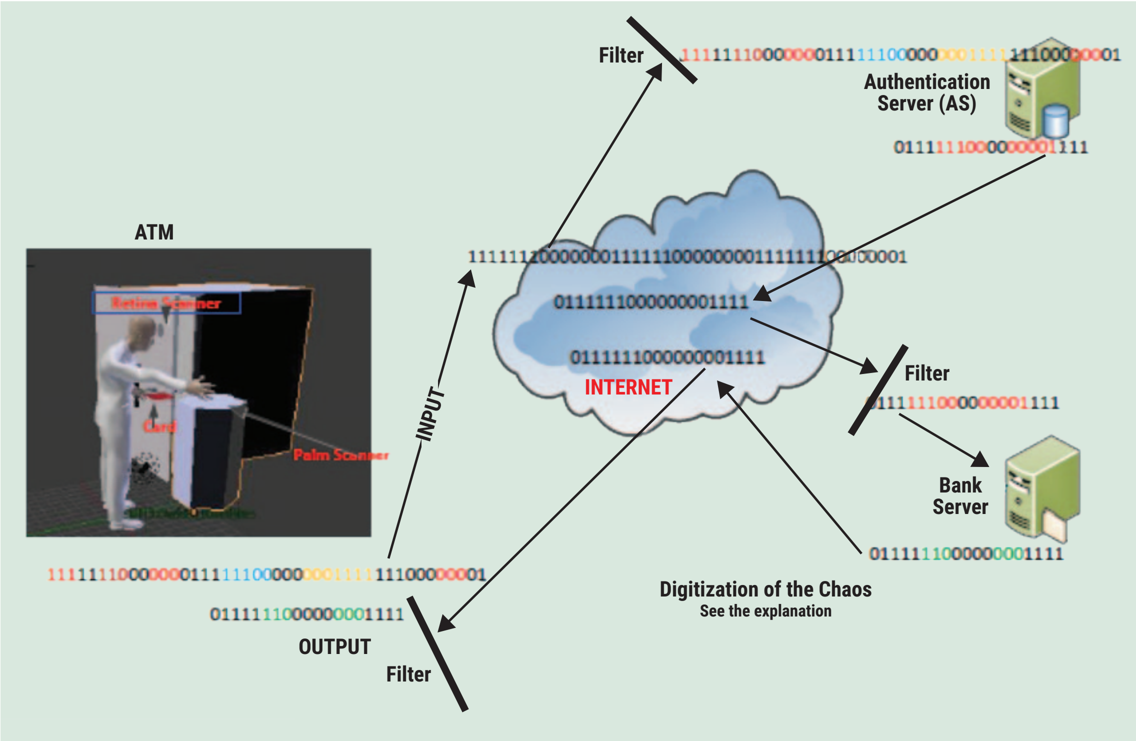
Using the researchers' proposed card to make a withdrawal from an automatic teller machine (ATM) is a simple example to show the computer's chaos-theory functionality.

Figure 1 shows how the researchers' proposed red card (next to the person's left hand) is used to make an ATM withdrawal:

- The input is the customer-entered data (black bits). Other data (colored bits) are added to the transaction (card physical characteristics, a customer's genetic and biometric data, and ATM location data).
- The data are transmitted through the Internet as usual (black bits). Anyone in the middle who analyzes the flow through the Internet cannot determine which bits come from the customer and which bits pertain to biometric data or come from the card or the customer imprint.
- After data arrive at the AS, a filter sorts the information by analyzing each bit according to its frequency (color). This operation allows the AS to authenticate the customer and to transmit to the bank server (BS) the data coming from the ATM and entered by the customer.
- The bank server recognizes the customer and ATM data and approves the transaction by adding some information (green bits) to the response. The transaction is transmitted as usual through the Internet (bits in black).

© 2019 ISACA. All rights reserved. *www.isaca.org*

Figure 1—ATM Card Withdrawal Using Chaos Theory Cybersecurity



- In the output, a filter recovers the original color of each bit and the ATM releases the card and the cash to the customer.

Note two important things about this example transaction:

1. The biometric and genetic data are only processed through a government authentication server. (The AS must be a government authentication server.)
2. Throughout the transaction, a physical contact is maintained between the ATM and the AS, and between the ATM and the BS with a laser. Any attempt to suspend this contact by removing the card will cancel the transaction.

“ UNLIKE EXISTING SYSTEMS, THE PROBABILITY OF IMPUNITY (COMMITTING FRAUD AND GOING UNNOTICED) BECOMES ALMOST NIL WITH THE PROPOSED SYSTEM. ”

Conclusion

All the tools (e.g., algorithms, circuits) to realize this digital card are currently under study. Theoretically, some are already designed. This card is designed to protect the user against identity theft and counterfeiting. It uses unique and inviolable data. The card's imprint, the spatio-temporal landmarks, and the genetic and biometric data of the owner are closely linked. By backing up these data on centralized authentication servers and on the card, the biometric and genetic data of the user are prevented from being in the wild or being handled dishonestly or uncontrollably by unauthorized and unknown people. Some say that the proposed system will never be tamperproof, but its goal is not to eradicate cybercrime. The goal of the system is to reduce fraud. Someone who threatens another person with a weapon until having the victim scan his or her fingerprints does not commit a fraud, but

© 2019 ISACA. All rights reserved. *www.isaca.org*

a crime. The infatuation with unjust enrichment and the search for some unhealthy notoriety will always entice some daredevils to take their chance. In opposition to existing systems showing signs of flaws, the proposed project may become more accurate in deterring fraud. Unlike existing systems, the probability of impunity (committing fraud and going unnoticed) becomes almost nil with the proposed system, and building systems with chaos theories in mind can help reduce the likelihood of fraud.

Endnotes

[1] Professor Messer, "The OSI Model – CompTIA Network+ N10-004: 4.1," YouTube.com, 18 July 2010, *https://www.youtube.com/watch?v=W438koUR04o*

[2] Yash Rawat, "The Story of Maths 1 of 4 the Language of the Universe," YouTube.com, 13 August 2015, *https://www.youtube.com/watch?v=mJbChZrXDJE*

© 2019 ISACA. All rights reserved. *www.isaca.org*